

EXHIBIT 1

Google is experimenting with new ways of supporting the delivery and measurement of digital advertising in ways that better protect people's privacy online via Chrome's [Privacy Sandbox](#) initiative. Users that participate in Chrome's Privacy Sandbox Origin Trials may see relevant ads from Google based on [Topics](#) or [FLEDGE](#) data stored on, or shared with, their browser. Google may also measure ad performance using [Attribution Reporting](#) data stored on, or shared with, their browsers. [More information on the Privacy Sandbox](#).

HOW GOOGLE USES INFORMATION FROM SITES OR APPS THAT USE OUR SERVICES

Many websites and apps use Google services to improve their content and keep it free. When they integrate our services, these sites and apps share information with Google.

For example, when you visit a website that uses advertising services like AdSense, including analytics tools like Google Analytics, or embeds video content from YouTube, your web browser automatically sends certain information to Google. This includes the URL of the page you're visiting and your IP address. We may also [set cookies on your browser](#) or read cookies that are already there. Apps that use Google advertising services also share information with Google, such as the name of the app and a unique identifier for advertising.

Google uses the information shared by sites and apps to deliver our services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on our partners' sites and apps. See our [Privacy Policy](#) to learn more about how we process data for each of these purposes and our [Advertising](#) page for more about Google ads, how your information is used in the context of advertising, and how long Google stores this information.

Our [Privacy Policy](#) explains the legal grounds Google relies upon to process your information — for example, we may process your information with your consent or to pursue legitimate interests such as providing, maintaining and improving our services to meet the needs of our users.

Sometimes, when processing information shared with us by sites and apps, those sites and apps will ask for your consent before allowing Google to process your information. For example, a banner may appear on a site asking for consent for Google to process the information that site collects. When that happens, we will respect the purposes described in the consent you give to the site or app, rather than the legal grounds described in the Google Privacy Policy. If you want to change or withdraw your consent, you should visit the site or app in question to do so.

Ad personalization

If ad personalization is turned on, Google will use your information to make your ads more useful for you. For example, a website that sells mountain bikes might use Google's ad services. After you visit that site, you could see an ad for mountain bikes on a different site that shows ads served by Google.

If ad personalization is off, Google will not collect or use your information to create an ad profile or personalize the ads Google shows to you. You will still see ads, but they may not be as useful. Ads may still be based on the topic of the website or app you're looking at, your current search terms, or on your general location, but not on your interests, search history, or browsing history. Your information can still be used for the other purposes mentioned above, such as to measure the effectiveness of advertising and protect against fraud and abuse.

When you interact with a website or app that uses Google services, you may be asked to choose whether you want to see personalized ads from ad providers, including Google. Regardless of your choice, Google will not personalize the ads you see if your ad personalization setting is off or your account is ineligible for personalized ads.

You can see and control what information we use to show you ads by visiting your [ad settings](#).

How you can control the information collected by Google on these sites and apps

Here are some of the ways you can control the information that is shared by your device when you visit or interact with sites and apps that use Google services:

- [Ad Settings](#) helps you control ads you see on Google services (such as Google Search or YouTube), or on non-Google websites and apps that use Google ad services. You can also [learn how](#) ads are personalized, opt out of ad personalization, and block specific advertisers.
- If you are signed in to your Google Account, and depending on your Account settings, [My Activity](#) allows you to review and control data that's created when you use Google services, including the information we collect from the sites and apps you have visited. You can browse by date and by topic, and delete part or all of your activity.
- Many websites and apps use Google Analytics to understand how visitors engage with their sites or apps. If you don't want Analytics to be used in your browser, you can [install the Google Analytics browser add-on](#). Learn more about [Google Analytics and privacy](#).
- [Incognito mode in Chrome](#) allows you to browse the web without recording webpages and files in your browser or Account history (unless you choose to sign in). Cookies are deleted after you've closed all of your incognito windows and tabs,

and your bookmarks and settings are stored until you delete them. Learn more about [cookies](#).

- Many browsers, including Chrome, allow you to block third-party cookies. You can also clear any existing cookies from within your browser. Learn more about [managing cookies in Chrome](#).

EXHIBIT 2

**Sealed in its
Entirety**

EXHIBIT 3

Sealed Entirely

EXHIBIT 4



Create an Account

Your Google Account gives you access to Gmail and [other Google services](#). If you already have a Google Account, you can [sign in here](#).

Get started with Gmail

First name:

Last name:

Desired Login Name: @gmail.com
Examples: JSmith, John.Smith

Choose a password: [Password strength:](#)

Minimum of 8 characters in length.

Re-enter password:

☒ Stay signed in

☒ Enable Web History [Learn More](#)

Security question:

If you forget your password we will ask for the answer to your security question. [Learn More](#)

Answer:

Recovery email:

This address is used to authenticate your account should you ever encounter problems or forget your password. If you do not have another email address, you may leave this field blank. [Learn More](#)

Location:

Birthday:

MM/DD/YYYY (e.g. "8/29/2011")

Word Verification: Type the characters you see in the picture below.

Letters are not case-sensitive

Terms of Service: Please check the Google Account information you've entered above (feel free to change anything you like), and review the Terms of Service below.

With Gmail, you won't see blinking banner ads. Instead, we display ads you might find useful that are relevant to the content of your messages. [Learn more](#)

[Printable Version](#)

Google Terms of Service

Welcome to Google!

1. Your relationship with Google

By clicking on 'I accept' below you are agreeing to the [Terms of Service](#) above and both the [Program Policy](#) and the [Privacy Policy](#).

EXHIBIT 5

Create your Google Account

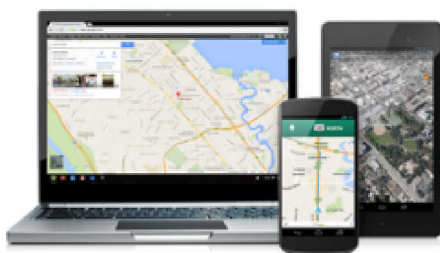
One account is all you need

A single username and password gets you into everything Google.



Take it all with you

Switch between devices, and pick up wherever you left off.



Name

Choose your username

[I prefer to use my current email address](#)

Create a password

Confirm your password

Birthday

Gender

Mobile phone

Your current email address

Prove you're not a robot



Skip this verification (phone verification may be required)

Location



I agree to the Google [Terms of Service](#) and [Privacy Policy](#)

[Next step](#)

[Learn more](#) about why we ask for this information.

EXHIBIT 6

Sealed Entirely

EXHIBIT 7

Privacy and Terms

You're in control of the data we
collect & how it's used

To create a Google Account, you'll need to agree to the [Terms of Service](#) below.

In addition, when you create an account, we process your information as described in our [Privacy Policy](#), including these key points:

Data we process when you use Google

- When you set up a Google Account, we store information you give us like your name, email address, and telephone number.
- When you use Google services to do things like write a message in Gmail or comment on a YouTube video, we store the information you create.
- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

Why we process it

We process this data for the purposes described in [our policy](#), including to:

- Help our services deliver more useful, customized content such as more relevant search results;
- Improve the quality of our services and develop new ones;
- Deliver personalized ads, depending on your account settings, both on Google services and on sites and apps that partner with Google;
- Improve security by protecting against fraud and abuse; and
- Conduct analytics and measurement to understand how our services are used. We also have partners that measure how our services are used. [Learn more](#) about these specific advertising and measurement partners.

Combining data

Why we process it

We process this data for the purposes described in [our policy](#), including to:

- Help our services deliver more useful, customized content such as more relevant search results;
- Improve the quality of our services and develop new ones;
- Deliver personalized ads, depending on your account settings, both on Google services and on sites and apps that partner with Google;
- Improve security by protecting against fraud and abuse; and
- Conduct analytics and measurement to understand how our services are used. We also have partners that measure how our services are used. [Learn more](#) about these specific advertising and measurement partners.

Combining data

We also combine this data among our services and across your devices for these purposes. For example, depending on your account settings, we show you ads based on information about your interests, which we can derive from your use of Search and YouTube, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

You're in control

Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data now by clicking "More Options" below. You can always adjust your controls later or withdraw your consent for the future by visiting My Account (myaccount.google.com).

[MORE OPTIONS](#)[Cancel](#)[I agree](#)

EXHIBIT 8



Privacy and Terms

MORE OPTIONS

Customize your Google experience by confirming your personalization settings and the data stored with your account.

You can always learn more about these options, adjust them, and review your activity in your Google Account (account.google.com).



Web & App Activity

Saves your activity on Google sites and apps, including searches and associated info like location. Also saves activity from sites, apps, and devices that use Google services, including Chrome history. This helps Google provide better search results, suggestions, and personalization across Google services.



Save my Web & App Activity in my



You're in control of the data we collect & how it's used


English (United States) ▼

[Help](#)

[Privacy](#)

[Terms](#)

[Dogfood feedback](#)



Privacy and Terms

personalization across Google services.

☒ Save my Web & App Activity in my Google Account


☐ Don't save my Web & App Activity in my Google Account

[Learn more](#)

☐ **Ads Personalization**

Google can show you ads based on your activity on Google services (such as Search or YouTube), and on websites and apps that partner with Google.


☒ Show me personalized ads



You're in control of the data we collect & how it's used

English (United States) ▼

[Help](#) [Privacy](#) [Terms](#) [Dogfood feedback](#)




Privacy and Terms

☒ Show me personalized ads

☐ Show me ads that aren't personalized

[Learn more](#)




YouTube Search History

Saves what you search for on YouTube to make your future searches faster and to give you better recommendations in YouTube and other Google services.

☒ Save my YouTube Search History in my Google Account


☐ Don't save my YouTube Search History in my Google Account



You're in control of the data we collect & how it's used


English (United States) ▼

[Help](#) [Privacy](#) [Terms](#) [Dogfood feedback](#)



Privacy and Terms


my Google Account

**YouTube Watch History**

Saves what you watch on YouTube to give you better recommendations in YouTube and other Google services.

☒ Save my YouTube Watch History in my Google Account

☐ Don't save my YouTube Watch History in my Google Account

**Location History**

Saves a private map of where you go with your signed-in devices (even when you're not actively using a Google product) to give you

You're in control of the data we collect & how it's used

English (United States) ▼ Help Privacy Terms [Dogfood feedback](#)



Privacy and Terms

signed-in devices (even when you're not actively using a Google product) to give you better map searches, commute routes, and more.

☐ Save my Location History in my Google Account

☒ Don't save my Location History in my Google Account

[Learn more](#)



Voice & Audio Activity

Saves a recording of your voice and audio input to help Google recognize your voice and improve speech recognition.



You're in control of the data we collect & how it's used

English (United States) ▼

[Help](#)

[Privacy](#)

[Terms](#)

[Dogfood feedback](#)



Privacy and Terms

Saves a recording of your voice and audio input to help Google recognize your voice and improve speech recognition.

☐ Save my Voice & Audio Activity in my Google Account

☒ Don't save my Voice & Audio Activity in my Google Account

[Learn more](#)

☐ Send me occasional reminders about these settings

These settings apply wherever you are signed in to your new Google Account.

[Cancel](#)

[I agree](#)

You're in control of the data we collect & how it's used

English (United States) ▼

[Help](#)

[Privacy](#)

[Terms](#)

[Dogfood feedback](#)

EXHIBIT 9

**Sealed in its
Entirety**

EXHIBIT 10

**Sealed in its
Entirety**

EXHIBIT 11

Privacy and Terms

By choosing “I agree” below you agree to Google’s [Terms of Service](#).

You also agree to our [Privacy Policy](#), which describes how we process your information, including these key points:

Data we process when you use Google

- When you set up a Google Account, we store information you give us like your name, email address, and telephone number.
 - When you use Google services to do things like write a message in Gmail or comment on a YouTube video, we store the information you create.
 - When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including information like the video you watched, device IDs, IP addresses, cookie data, and location.
 - We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.
- Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data at My Account (myaccount.google.com).

Why we process it

We process this data for the purposes described in [our policy](#), including to:

- Help our services deliver more useful, customized content such as more relevant search results;
- Improve the quality of our services and develop new ones;
- Deliver personalized ads, both on Google services and on sites and apps that partner with Google;
- Improve security by protecting against fraud and abuse; and
- Conduct analytics and measurement to understand how our services are used.

Combining data

We also combine data among our services and across your devices for these purposes. For example, we show you ads based on information from your use of Search and Gmail, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

[Cancel](#)

[I agree](#)

EXHIBIT 12

**Sealed in its
Entirety**

EXHIBIT 13

**Sealed in its
Entirety**

EXHIBIT 14

Privacy and Terms

To create a Google Account, you'll need to agree to the [Terms of Service](#) below.

In addition, when you create an account, we process your information as described in our [Privacy Policy](#), including these key points:

Data we process when you use Google

- When you set up a Google Account, we store information you give us like your name, email address, and telephone number.
- When you use Google services to do things like write a message in Gmail or comment on a YouTube video, we store the information you create.
- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

Why we process it

We process this data for the purposes described in [our policy](#), including to:

- Help our services deliver more useful, customized content such as more relevant search results;
- Improve the quality of our services and develop new ones;
- Deliver personalized ads, depending on your account settings, both on Google services and on sites and apps that partner with Google;
- Improve security by protecting against fraud and abuse; and
- Conduct analytics and measurement to understand how our services are used. We also have partners that measure how our services are used. [Learn more](#) about these specific advertising and measurement partners.

Combining data

We also combine this data among our services and across your devices for these purposes. For example, depending on your account settings, we show you ads based on information about your interests, which we can derive from your use of Search and YouTube, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

You're in control

Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we

collect and use this data now by clicking “More Options” below. You can always adjust your controls later or withdraw your consent for the future by visiting My Account (myaccount.google.com).

[MORE OPTIONS](#)

Cancel

I agree

EXHIBIT 15



**Sealed in its
Entirety**

EXHIBIT 16

Browse in private

If you don't want Google Chrome to remember your activity, you can browse the web privately in Incognito mode.

[Computer](#) [Android](#) [iPhone & iPad](#)

1. On your computer, open Chrome.
2. At the top right, click More  > **New Incognito Window**.
3. A new window appears. In the top corner, check for the Incognito icon .

You can also use a keyboard shortcut to open an Incognito window:

- Windows, Linux, or Chrome OS: Press **Ctrl + Shift + n**.
- Mac: Press **⌘ + Shift + n**.

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.



You can also choose to block third-party cookies when you open a new incognito window. [Learn more about cookies](#).

Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
 - **Windows or Chrome OS:** At the top right, click Close .
 - **Mac:** At the top left, click Close .

What happens when you browse privately

- Chrome won't save your browsing history, cookies and site data, or information entered in forms.
- Files you download and bookmarks you create will be kept.
- Your activity isn't hidden from websites you visit, your employer or school, or your internet service provider.

Learn more about [how private browsing works](#).

Related articles

- [How private browsing works](#)
 - [Let others browse Chrome as a guest](#)
 - [Clear Chrome browsing data](#)
-

EXHIBIT 17

**Sealed in its
Entirety**

EXHIBIT 18

How private browsing works in Chrome

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode. You can choose to block third-party cookies when you open a new incognito window. [Learn more about cookies.](#)

What happens when you browse privately

Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won't save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

- Websites you visit, including the ads and resources used on those sites
- Websites you sign in to
- Your employer, school, or whoever runs the network you're using
- Your internet service provider
- Search engines
 - Search engines may show search suggestions based on your location or activity in your current Incognito browsing session. When you search on Google, Google will always estimate the general area that you're searching from. [Learn more about location when you search on Google.](#)

Some of your info might still be visible

A web service, website, search engine, or provider may be able to see:

- Your IP address, which can be used to identify the general area you're in
- Your activity when you use a web service
- Your identity if you sign in to a web service, like Gmail

You can still find and use your payment, password and contact info, but you can't change your saved info in a Chrome Incognito window.

Downloads and bookmarks are saved

Chrome won't store the files you download while browsing in private. But, they're still saved to your Downloads folder, even after you exit Incognito. You and anyone who uses your device can see and open the files.

All bookmarks you create are saved to Chrome.

Some of your preferences, including accessibility choices and bookmark settings, may also be saved to Chrome.



You can also choose to block third-party cookies when you open a new incognito window. [Learn more about cookies.](#)

Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
 - **Windows or Chrome OS:** At the top right, click Close .
 - **Mac:** At the top left, click Close .

Related articles

- [Browse in private](#)
 - [Let others browse Chrome as a guest](#)
 - [Clear Chrome browsing data](#)
-

EXHIBIT 19

Google Chrome Privacy Whitepaper

Last modified: September 30, 2020 (Current as of Chrome 84.0.4147.135)

Omnibox | Network predictions | Search locale | New Tab page | Touch to Search | Search with Google Lens | Safe Browsing protection | Safety Check | Unwanted software protection | Offline Indicator | Google update | Network time | Counting install | Measuring promotions | Usage stats | Google Surveys | Spelling suggestions | Translate | Image Descriptions | Signing In | Autofill | Payments | Geolocation | Speech to text | Google Assistant on Chrome OS devices | Google Assistant on Android devices | Cloud Print | SSL certificate error reporting | Installed apps | Push Messaging | Chrome custom tabs | Continue where you left off | Chrome variations | Do Not Track | Plugins | Media licenses | MediaDrm provisioning | Cloud policy | Lite Mode (Chrome mobile) | Kid’s Google Account | Incognito and Guest mode | Handoff support | Security key | Physical web | Bluetooth | Data sent by Android | Integration with Digital Wellbeing |

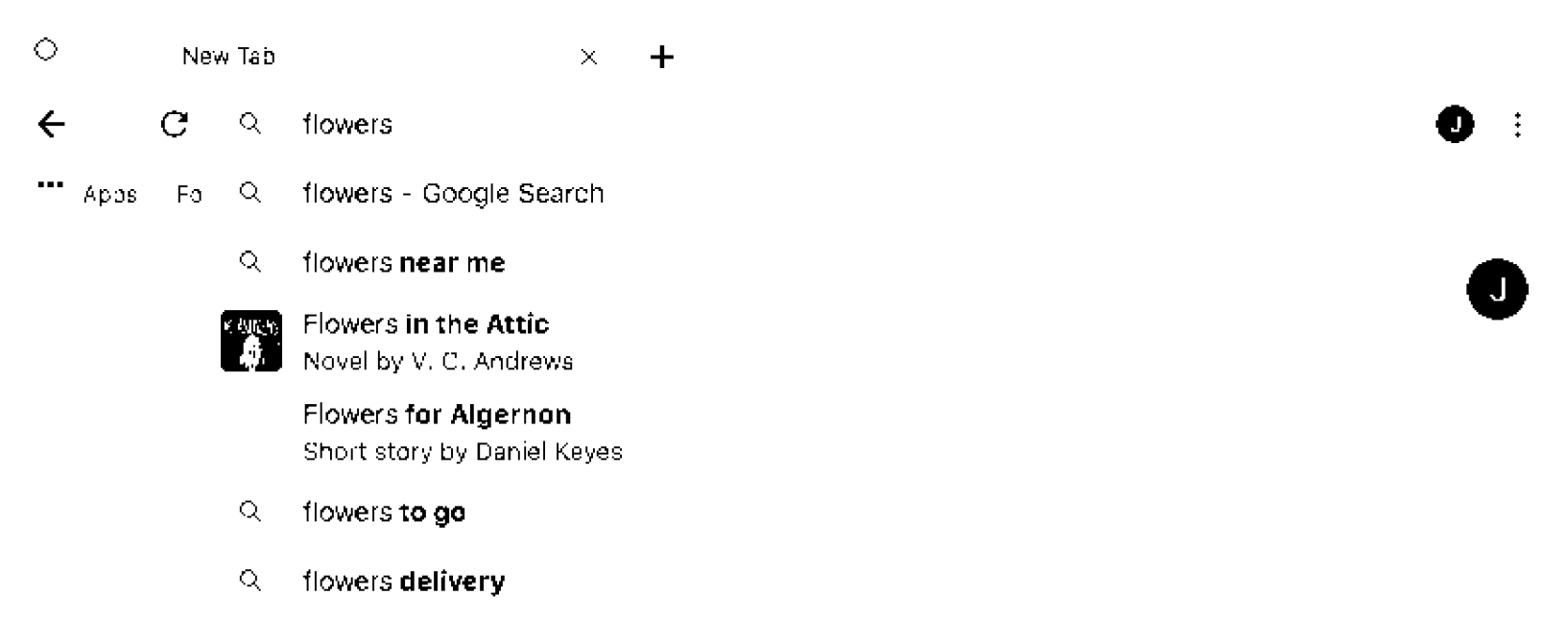
This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine). This document also describes the controls available to you regarding how your data is used by Chrome. Here we’re focusing on the desktop version of Chrome; we touch only tangentially on Chrome OS and Chrome for Mobile. This document does not cover features that are still under development, such as features in the beta, dev and canary channel and active field trials, or Android apps on Chrome OS if Play Apps are enabled.

If you have a question about Google Chrome and Privacy that this document doesn’t answer, please feel free to ask it in the [Community Forum](#). If you want to report a privacy issue, you can file it in [our public bug tracker](#). For issues that include confidential information, please use [this link](#). We’d be happy to hear from you.

Omnibox

Google Chrome uses a combined web address and search bar (we call it the “omnibox”) at the top of the browser window.

As you use the omnibox, your default search engine can suggest addresses and search queries that may be of interest to you. These suggestions make navigation and searching faster and easier, and are turned on by default. They can be turned off by unchecking "Autocomplete searches and URLs" in the “Sync and Google services” section of Chrome's settings.



When not in Incognito mode, in order to provide these suggestions, Chrome sends the text you've typed into the omnibox, along with a general categorization (e.g., "URL", "search query", or "unknown"), to your default search engine. Chrome will also send a signal to your default search engine when you focus in the omnibox, telling it to get ready to provide suggestions. That signal includes the URL of the currently displayed search engine results page. Your IP address and certain cookies are also sent to your default search engine with all requests, in order to return the results that are most relevant to you.

To provide suggestions and search results faster, Chrome may preconnect to your default search engine in the background. Chrome will not preconnect if you have either turned off “Preload pages for faster browsing and searching” in the “Cookies” part of “Privacy and security” section or "Autocomplete searches and URLs" in the “Sync and Google services” section of Chrome's settings. When Chrome preconnects, it resolves the search engine’s IP address and connects it to the search engine, exposing your IP address.

When in Incognito mode, in order to provide these suggestions, Chrome relies on an on-device model that does not communicate with your default search engine until you select a suggestion.

If Chrome determines that your typing may contain sensitive information, such as authentication credentials, local file names, or URL data that is normally

If Google is your default search engine, when you select one of the omnibox suggestions, Chrome sends your original search query, the suggestion you selected, and the position of the suggestion back to Google. This information helps improve the quality of the suggestion feature, and it's logged and anonymized in the same manner as Google web searches. Logs of these suggestion requests are retained for two weeks, after which 2% of the log data is randomly selected, anonymized, and retained in order to improve the suggestion feature.

If you've chosen to sync your Chrome history, and if Google is your default search engine, the URL of the page you're viewing is sent to Google in order to provide better, contextually relevant suggestions. URLs are sent only for HTTP pages and HTTPS pages, not other schemes such as file: and ftp:. Additionally, Chrome may present website and search query suggestions as soon as you place the cursor in the omnibox, before you start typing. Chrome is in the process of transitioning to a new service to provide these on-focus suggestions. For most users on desktop versions of Chrome, the request and complete set of suggestions are retained on Google servers in order to further improve and personalize the feature. When the URL that triggered the set of suggestions is deleted from your history, the set of suggestions will stop influencing suggestions personalized to you, and will be deleted; otherwise they are retained in your Google account for a year. For a small portion of users on desktop versions of Chrome, and users on mobile versions of Chrome, the logging described in the previous paragraphs apply except that URLs are never included in the 2% sampling of log data.

On Android, your location will also be sent to Google via an X-Geo HTTP request header if Google is your default search engine, the Chrome app has the permission to use your geolocation, and you haven't blocked geolocation for www.google.com (or country-specific origins such as www.google.de). Additionally, if your device has network location enabled (High Accuracy or Battery Saving Device Location mode in Android settings), the X-Geo header may also include visible network IDs (WiFi and Cell), used to geocode the request server-side. The X-Geo header will never be sent in Incognito mode. HTTPS will be required to include this header in the request. You can learn more about how to control the Android OS location sharing with apps on [this article](#) for Nexus, or find your device [here](#) if you do not use a Nexus. How to control location sharing with a site within Chrome is written in [this article](#). See the [Geolocation](#) section of this whitepaper for more information on default geolocation permissions.

Additionally, if Google is your default search engine and you have enabled sync, omnibox may also show suggestions for your Google Drive files. You can turn this functionality off by disabling the "Drive suggestions" option in the "Sync and Google services" section of Chrome's settings.

If you use a non-Google search provider as your default search engine, queries are sent and logged under that provider's privacy policy.

Additionally, when you use the omnibox to search for a single word, Chrome may send this word to your DNS server to see whether it corresponds to a host on your network, and may try to connect to the corresponding host. This gives you the option to navigate to that host instead of searching. For example, if your router goes by the hostname "router", and you type "router" in the omnibox, you're given the option to navigate to <https://router/>, as well as to search for the word "router" with your default search provider. This feature is not controlled by the "Use a prediction service to help complete searches and URLs..." option because it does not involve sending data to your default search engine.

Network predictions

Chrome uses a service to predict which resources and pages are likely to be needed next in order to load pages more quickly. The prediction service uses navigation history, local heuristics, and data learned from Google's search crawlers. Retrieving the data from Google's crawlers requires sending the URL of the current page to Google, and so it is only used if you've opted into "Make Searches and Browsing Better (Sends URLs of the pages you visit to Google)" and/or enabled Lite Mode. The prediction service may initiate actions such as DNS prefetching, TCP and TLS preconnection, and prefetching of web pages. To [turn off](#) network predictions, uncheck "Preload pages for faster browsing and searching" in the "Privacy and security > Cookies" section of Chrome's settings on desktop, in the "Privacy" section of Chrome's settings on Android, and in the "Bandwidth" section of Chrome's settings on iOS.

To improve load times, the browser can be asked to prefetch links that you might click next. Chrome supports five types of prefetching:

- Chrome prefetching - can be initiated by Chrome itself whenever it detects a search query typed in the omnibox, a likely beginning of a URL you type often in the omnibox, or when you have Lite mode enabled and are visiting Google Search.
- Webpage prefetching - requested by one web page to prefetch another
- AMP prefetching - can be requested only by the Google Search App on Android to prefetch several accelerated mobile pages (AMP) articles and display them later in a Chrome Custom Tab
- CustomTabs prefetching - any Android app can request to prefetch several URLs to speed up displaying them later in a Chrome Custom Tab
- Privacy-preserving search result link prefetching - for Lite mode users

Controlling the feature. All prefetching types except webpage prefetching are controlled by Chrome's prediction service setting. Webpage prefetching is allowed regardless of whether Chrome's network prediction service feature is enabled.

Handling of cookies. Except for the Lite mode-only prefetching case, the prefetched site is allowed to set and read its own cookies even if you don't end up visiting the prefetched page, and prefetching is disabled if you have chosen to block third-party cookies. In the Lite mode-only case, prefetching is disabled if you have a cookie for the site, and the site can only set a cookie once you click on the link that was prefetched (see the [Lite mode](#) section for more details).

Javascript execution. For AMP prefetching the page is fully rendered and Javascript is also executed. For the remaining types of prefetching Javascript is not executed.

If Google is set as your default search engine, Chrome will try to determine the most appropriate locale for Google search queries conducted from the omnibox in order to give you relevant search results based on your location. For example, if you were in Germany, your omnibox searches may go through google.de instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTPS request to google.com would be (see the description of “server logs” in the privacy key terms for details). If you do not have any cookies from google.com, this request will not create any.

New Tab page

The Chrome New Tab page may display suggestions for websites that you might want to visit.

In order to help you get started, Chrome may suggest content that is popular in your country or region. Chrome uses your IP address to identify your country or region.

Chrome tries to make personalized suggestions that are useful to you. For this, Chrome uses the sites you have visited from your local browsing history. On Android, the most popular languages of the sites you visited may also be sent to Google to provide suggestions in languages you prefer to read, and the device display DPI may be sent to format content for your device. To save data, Chrome may additionally send a hash of the content that Google provided to you the last time, so that you only download content when there is something new.

If you are signed into Chrome, suggestions are *also* based on data stored in your Google account activity. You can control the collection of data in your Google account at Activity controls and manage your account activity at My Activity. For example, if you sync your browsing history and have enabled its use in your Web & App activity, Google may suggest sites that relate to sites you have visited in the past. Chrome measures the quality of suggestions by sending Google information about the sets of suggestions that were displayed, and those that were selected.

On the desktop version of Chrome, you may also manually add shortcuts to websites that you regularly visit, or edit Chrome’s existing website suggestions. After you add, edit, or delete a shortcut to a website, the Chrome New Tab page will not suggest any new websites to you.

Suggestions generated from your browsing history will be removed once you clear your browsing history. However, if you customized your suggestions, they will not be removed.

For Chrome on Android, in certain countries, Chrome may download the content of the New Tab page suggestions from Google, for use while offline. Chrome sends to Google a cookieless request with the URL for each suggestion, along with Chrome’s user agent string, in order to render the content. You can remove downloaded content by clearing Chrome’s cache data, or by opening the Downloads menu and selecting individual pages to delete. You can disable this feature by disabling “Download articles for you on Wi-Fi” in Chrome’s Downloads settings.

For Chrome on Android, if you’re signed in to Chrome, your preferences for the suggested articles can be modified or removed using the “Manage Interests” option from the three dots menu. Your preferences will be sent to Google so that better suggestions are provided to you in the future. For example, if you indicate that you’re not interested in a particular topic or publisher, suggestions about that topic or publisher will not be shown in the future. Likewise, you can indicate that you’re not interested in a specific article via the “Hide story” option in the article’s three dots menu. Suggestions are also personalized based on your interactions with the suggested articles (for example, tapping on or ignoring an article). You can manage this interaction data, which is stored in the Discover section of your Google account, at My Activity.

For desktop and Android versions of Chrome, when you open a new tab, Chrome loads a New Tab page customized by your default search engine (e.g., google.com) if it’s available. This page is preloaded in the background and refreshed periodically so that it opens quickly. Your IP address and cookies, as well as your current browser theme, are sent to your search engine with each refresh request so that the New Tab page can be correctly displayed. See the Embedded Search API for more details. Your search engine may also record your interactions with the New Tab page.

The New Tab page content may be designed by your default search provider. Suggested websites are embedded by Chrome into the New Tab page in a way that does not expose them to your default search provider.

If your default search provider is Google, the New Tab page also contains a web address and search bar that behaves like the omnibox.

This information about the New Tab page may not apply if you've installed an extension that overrides the New Tab page.

Touch to Search

When you select a word, the word, the surrounding text, the languages you speak (from Chrome's Languages settings), and the home country of your device's SIM card are sent to Google to identify recommended search terms (for example, selecting "whale" on a site about the blue whale would lead to the selection expanding to show "blue whale"). The selected word is logged in accordance with standard Google logging policies, and the surrounding text and home country are logged only when the page is already in Google's search index. If you have turned on “Make searches and browsing better”, the URL of the page is also sent and logged, and is used to improve your query suggestions.

When Google returns a search suggestion, a card appears that may present an action or additional information related to the search. Opening this card is considered a regular search and navigation on Google, so standard logging policies apply.

Adjusting a selection causes a search for the exact selection. For example, if the user selects "climate" and the selection is automatically expanded to "climate change", the user can adjust the selection back to just "climate" and opening the panel would show full search results for "climate" rather than "climate change". Saying “Ok Google” after selecting a word provides the word and its surrounding text as context for the Google Assistant.

Touch to Search is enabled in a limited mode by default: potentially privacy-sensitive data, such as the URL and surrounding text, is not sent for HTTPS pages. Touch to Search can be fully enabled and disabled in the card or in the Chrome privacy settings.

Search with Google Lens

On Android Chrome, if Google is selected as the default search engine and a recent version of the Google app is installed on your device, touching & holding on an image will present you with an option to initiate a search with Google Lens.

A tap on that menu item will redirect you to the Lens experience in the Google App and the image bytes of the selected image will be sent to the Google Lens app. For non-incognito users, the name of the currently signed-in account (if applicable), image tag attributes, and Chrome experiments may also be sent to the Google App. This information is used to improve the user experience within the Lens app.

Triggering a Lens search is considered a regular search and navigation on Google, so standard logging policies apply.

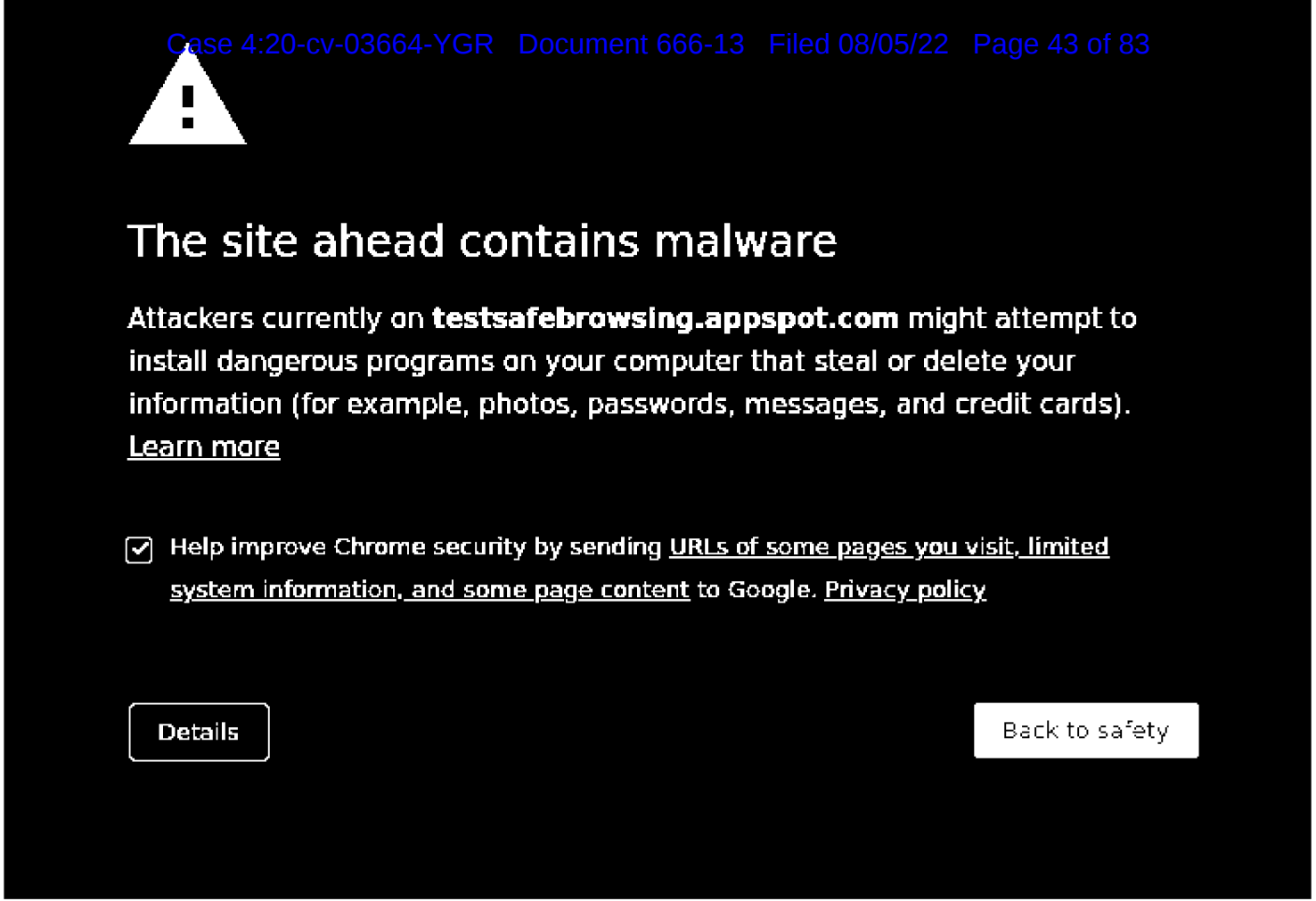
Safe Browsing protection

Google Chrome includes an optional feature called "Safe Browsing" to help protect you against phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. You can find more information at safebrowsing.google.com about how Safe Browsing protects you in Chrome and other Google products. Safe Browsing is designed specifically to protect your privacy and is also used by other popular browsers.

You can find settings for Safe Browsing in the “Privacy and security > Security” section of Chrome’s settings. When Safe Browsing is enabled in the “Standard protection” mode (pictured below), Chrome contacts Google's servers periodically to download the most recent Safe Browsing list of unsafe sites including sites associated with phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or Chrome extensions. The most recent copy of this list is stored locally on your system. Chrome checks the URL of each site you visit or file you download against this local list. If you navigate to a URL that appears on the list, Chrome sends a partial URL fingerprint (the first 32 bits of a SHA-256 hash of the URL) to Google for verification that the URL is indeed dangerous. Chrome also sends a partial URL fingerprint when a site requests a potentially dangerous permission, so that Google can protect you if the site is malicious. Google cannot determine the actual URL from this information.

In addition to the URL check described above, Chrome also conducts client-side checks. If a website looks suspicious, Chrome sends a subset of likely phishing and social engineering terms found on the page to Google, in order to determine whether the website should be considered malicious. Chrome can also help protect you from phishing if you type one of your previously saved passwords into an uncommon site. In this case Chrome sends the URL and referrers of the page to Google to see if the page might be trying to steal your password.

If you encounter a website that is on Chrome’s Safe Browsing list, you may see a warning like the one shown below.



You can [visit our malware warning test page](#) or [social engineering warning test page](#) to see the above example in action. For more information about the warning pages, see [Manage warnings about unsafe sites](#).

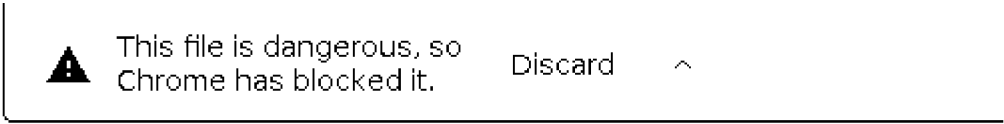
Additionally, if you've opted into “Make Searches and Browsing Better (sends URLs of the pages you visit to Google)”, Chrome sends a request to Safe Browsing each time you visit a page that isn’t in Chrome’s local list of safe sites in order to gather the latest reputation of that website (we call this mechanism “real-time checks”). If you sync your browsing history without a sync passphrase, this request also contains a temporary authentication token tied to your Google account to provide better protections to some users whose account may be under attack. If the website is deemed unsafe by Safe Browsing, you may see a warning like the one shown above. This mechanism is designed to catch unsafe sites that switch domains very quickly or hide from Google's crawlers. Pages loaded in Incognito are not checked using this mechanism.

You can also opt in to reporting additional [data relevant to security](#) to help improve Safe Browsing and security on the Internet. You can opt in by turning on the “Help improve security on the web for everyone” setting in the “Privacy and security > Security” section of Chrome's settings. You can also opt in from the warning page shown above. If you opt in, Chrome will send an incident report to Google every time you receive a warning, visit a suspicious page, and on a very small fraction of sites where Chrome thinks there could be threats, to help Safe Browsing learn about the new threats you may be encountering. Additionally, some downloaded files that are suspicious and show a warning may be sent to Google for investigation each time they are encountered. All reports are sent to Google over an encrypted channel and can include URLs, headers, and snippets of content from the page and they never include data from browsing you do in Incognito mode. If Chrome discovers unwanted or malicious software on your machine, the reports may also include details about malicious files and registry entries. This data is used only to improve Safe Browsing and to improve security on the Internet. For example, Chrome reports some [SSL certificate](#) chains to Google to help improve the accuracy of Chrome’s SSL warnings.

Please be aware that if you disable the Safe Browsing feature, Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software. We don't recommend turning it off.

If you are a webmaster, developer, or network admin, you can find more relevant information about Safe Browsing on [this page](#).

Safe Browsing also protects you from abusive extensions and malicious software. When Chrome starts, and on each update of the Safe Browsing list, Chrome scans extensions installed in your browser against the Safe Browsing list. If an extension on the list is found, Chrome will disable the extension, offer you relevant information and may provide an option for you to remove the extension or re-enable it. Chrome also sends the particular extension ID to Safe Browsing. Extensions can also be disabled by Chrome if they're determined to be malicious during an [update](#). If you attempt to download a file on Chrome’s Safe Browsing list, you'll see a warning like this one:



To warn you about potentially dangerous files, like the picture shown above, Chrome checks the URL of potentially dangerous file types you download against a list of URLs that have been verified. Potentially dangerous file types include both executables and commonly-abused document types. This list is stored locally on your computer and updated regularly. Chrome does not send information to Google for files you download from URLs in this list, or if the file is signed by a verified publisher. For all other unverified potentially dangerous file downloads, Chrome sends Google the information needed to help determine whether the download is harmful, including some or all of the following: information about the full URL of the site or file download, all related referrers and redirects, code signing certificates, file hashes, and file header information. Chrome may then show a warning like the one pictured above.

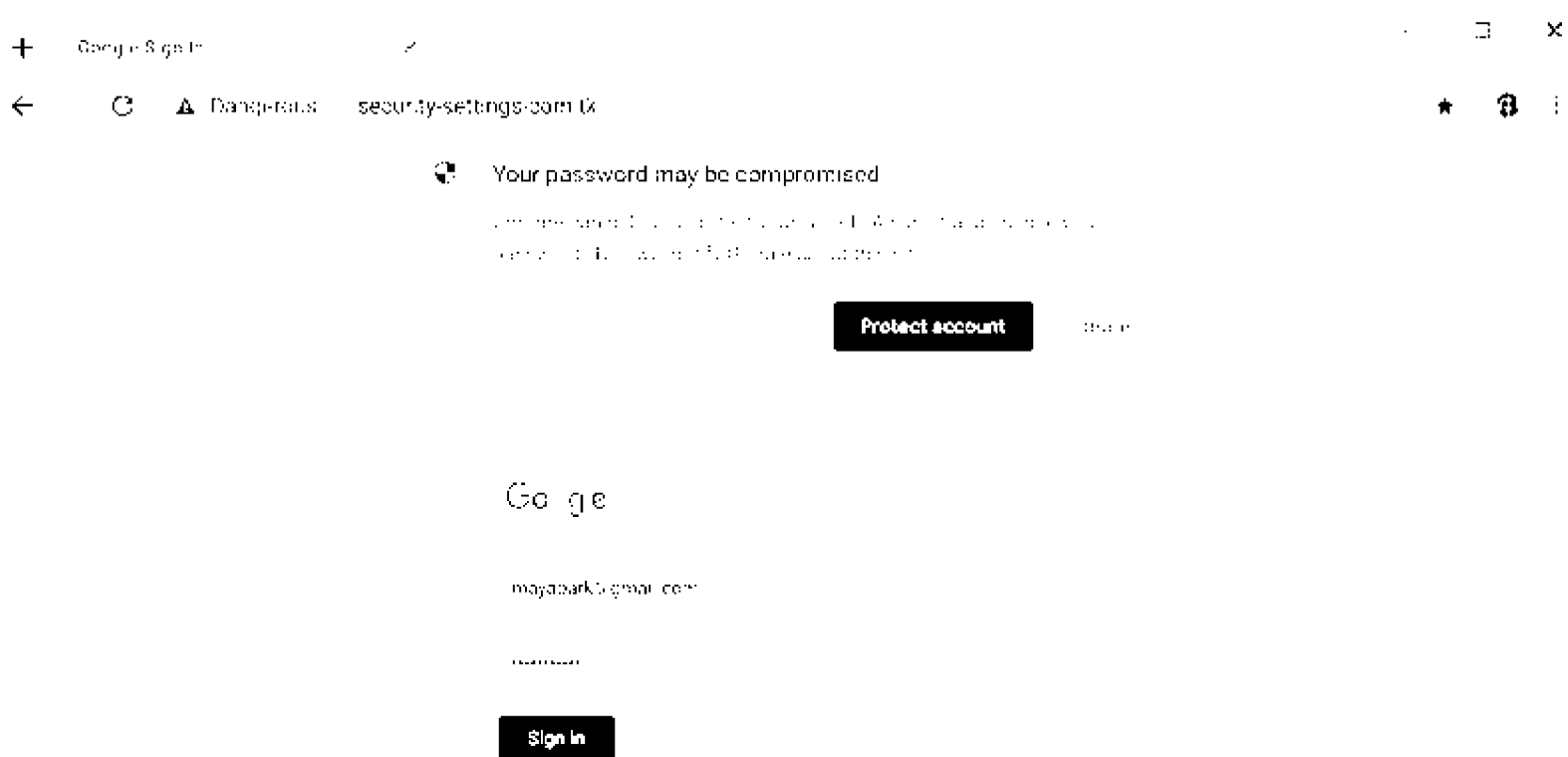
If you are enrolled in [Google's Advanced Protection Program](#), Chrome will show you additional warnings when you download files but where Safe Browsing is unable to ascertain they are safe.

Case 4:20-cv-03664-YGR Document 666-13 Filed 06/05/22 Page 44 of 83

Chrome helps protect you against password phishing by checking with Google when you enter your password on an uncommon page. Chrome keeps a local list of popular websites that Safe Browsing found to be safe. If Chrome detects that you have entered your Google account password or one of your passwords stored in Chrome’s password manager on a website that’s not on the list, it sends a request to Safe Browsing to gather the reputation of that website. The verdict received from Safe Browsing is usually cached on your device for 1 week. For users who have enabled the "Help improve security on the web for everyone" setting, Chrome will ignore the list of popular websites for a small fraction of visits, to test the accuracy of that list.

If the reused password is your Google account password and the verdict for the website is that it is phishing, Chrome will suggest that you change your Google account password to avoid losing access to your account.

If you sync your browsing history without a sync passphrase, or if you accept the “Protect account” option from the dialog shown below, Chrome sends a request to Google to protect your account. This request contains the URL where the phishing attempt happened, and the verdict received from Safe Browsing.



If you've opted into “Help improve security on the web for everyone”, Chrome also sends a request to Safe Browsing each time you start to enter a password on a page that isn’t in Chrome’s local list. In addition, the request Chrome sends to Safe Browsing to determine the reputation of the website on which you reuse your password includes the list of websites for which you saved this password in Chrome’s password manager (but not the password itself).

If Chrome detects that your settings have been tampered with, Chrome reports the URL of the last downloaded potentially dangerous file, and information about the nature of the possible tampering, to the Safe Browsing service.

Chrome asks your permission before using certain web features (APIs) that might have associated risks. Some sites trigger these permission requests in ways users find undesirable or annoying. On these sites Chrome may send the partial URL fingerprint to Google to verify if a less intrusive UI should be used to surface the request.

Enhanced protection

Faster, proactive protection against dangerous websites, downloads, and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.

Predicts and warns you about dangerous events before they happen

Keeps you safe on Chrome and may be used to improve your security in other Google apps when you are signed in

Improves security for you and everyone on the web

Warns you if passwords are exposed in a data breach

Sends URLs to Safe Browsing to check them. Also sends a small sample of pages, downloads, extension activity, and system information to help discover new threats. Temporarily links this data to your Google Account when you're signed in, to protect you across Google apps.

Standard protection

Standard protection against websites, downloads, and extensions that are known to be dangerous.

Detects and warns you about dangerous events when they happen

Checks URLs with a list of unsafe sites stored in Chrome. If a site tries to steal your password, or when you download a harmful file, Chrome may also send URLs, including bits of page content, to Safe Browsing.

Help improve security on the web for everyone

Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.

Warn you if passwords are exposed in a data breach

Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

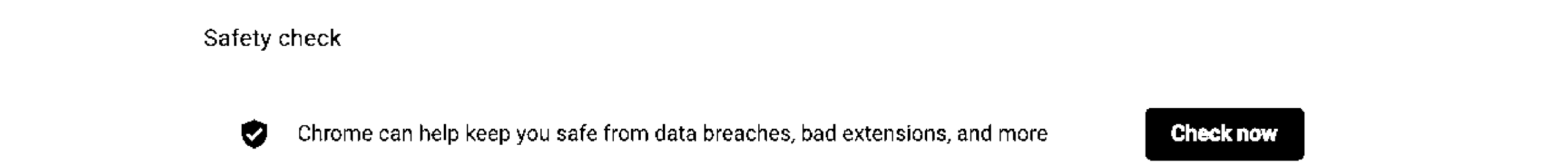
If you’ve opted into “Enhanced protection” (pictured above), in addition to all the protections described above for “Standard protection” mode, Chrome will use the real-time checks mechanism described above for checking the Safe Browsing reputation of top-level URLs and iframe URLs. If you're signed in to Chrome, the requests for performing real-time checks and the requests for checking potentially dangerous file downloads contain a temporary authentication token tied to your Google account that is used to protect you across Google apps. Enhanced protection also enables reporting additional data relevant to security to help improve Safe Browsing and overall web security, and it enables Chrome’s password breach detection. When browsing in incognito or guest mode, these extra checks do not occur, and Enhanced protection mode operates the same way as Standard protection.

For all Safe Browsing requests and reports, Google logs the transferred data in its raw form and retains this data for up to 30 days. Google collects standard log information for Safe Browsing requests, including an IP address and one or more cookies. After at most 30 days, Safe Browsing deletes the raw logs, storing only calculated data in an anonymized form that does not include your IP addresses or cookies. Additionally, Safe Browsing requests won’t be associated with your Google Account, except if the request includes the temporary authentication token described above. They are, however, tied to the other Safe Browsing requests made from the same device.

For Chrome on iOS 13 and later, Apple allows for connecting to multiple Safe Browsing services. This means that Chrome may connect to a third-party Safe Browsing service instead of the Google one. Apple determines which Safe Browsing service to connect to based on factors like your device locale.

Safety Check

GOOG-CABR-00048623



Unwanted software protection

The Windows version of Chrome is able to detect and remove certain types of software that violate [Google's Unwanted Software Policy](#). If left in your system, this software may perform unwanted actions, such as changing your Chrome settings without your approval. Chrome periodically scans your device to detect potentially unwanted software. In addition, if you have opted in to automatically report details of possible security incidents to Google, Chrome will report information about unwanted software, including relevant file metadata and system settings linked to the unwanted software found on your computer.

If you perform an unwanted software check on your computer from the Settings page, Chrome reports information about unwanted software and your system. System information includes metadata about programs installed or running on your system that could be associated with harmful software, such as: services and processes, scheduled tasks, system registry values commonly used by malicious software, command-line arguments of Chrome shortcuts, Windows proxy settings, and software modules loaded into Chrome or the network stack. You can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the scan.

If unwanted software is detected, Chrome will offer you an option to clean it up by using the Chrome Cleanup Tool. This will [quarantine](#) detected malicious files, delete harmful extensions and registry keys, and [reset](#) your settings. The Chrome Cleanup Tool also reports information about unwanted software and your system to Google, and again you can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the cleanup.

This data is used for the purpose of improving Google's ability to detect unwanted software and offer better protection to Chrome users. It is used in accordance with Google's [Privacy Policy](#) and is stored for up to 14 days, after which only aggregated statistics are retained.

Offline Indicator

On Android versions Lollipop and older, when Chrome detects a network change, it sends a cookieless request to http://connectivitycheck.gstatic.com/generate_204 or http://clients4.google.com/generate_204 to determine whether you're offline and display an offline indicator.

Software updates

Desktop versions of Chrome and the Google Chrome Apps Launcher use [Google Update](#) to keep you up to date with the latest and most secure versions of software. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is open source.

Google Update requests include information necessary for the update process, such as the version of Chrome, its release channel, basic hardware information, and update errors that have been encountered. The update requests also send Google information that helps us understand [how many people](#) are using Google Chrome and the Chrome Apps Launcher – specifically, whether the software was used in the last day, the number of days since the last time it was used, the total number of days it has been installed, and the number of active profiles. Google Update also periodically sends a non-unique four-letter tag that contains information about [how you obtained Google Chrome](#). This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is the same as everyone who obtained Google Chrome the same way.

Because Chrome OS updates the entire OS stack, Google Update on Chrome OS also sends the current Chrome OS version and hardware model information to Google in order to ensure that the correct software updates and hardware manufacturer customizations such as apps, wallpaper, and help articles are delivered. This information is not personally identifiable, and is common to all users of Chrome OS on the same revision of device.

Unlike the desktop versions of Chrome, the delivery and management of updates for mobile versions of Chrome are managed through the app stores for Android and iOS. Mobile versions of Chrome utilize the servers described above for [counting active installations](#).

Chrome extensions and applications that you've installed are kept up to date with a similar system used for updating desktop versions of Chrome. These update requests include similar information (such as the application ID, when the application was last used, and how long it's been installed). We use these requests to determine the aggregate popularity and usage of applications and extensions. If you are using an extension or application restricted to a certain audience,

authentication tokens are sent with the update requests for these add-ons. For security reasons, Chrome also occasionally sends a cookieless request to the Chrome Web Store, in order to verify that installed extensions and applications that claim to be from the store are genuine.

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which can be updated independently. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (e.g., "fmeadaodfnidclnjhlkdgjkolmhmfofk"). An update request for a component contains this ID, the hash of the previous download (called a "fingerprint"), and the component's version. Because every installation has the same ID, and downloads of the same component have the same fingerprint, none of this information is personally identifiable.

If you install web apps on an Android device, a Google server is responsible for creating a native Android package that can be verified for authenticity by Chrome. When Chrome is updated or notices that the web app's manifest has changed, Chrome asks the server for a new version of the Android package in a cookieless request. If the information needed to create the native Android package cannot be acquired by the server (e.g., because the information is behind a corporate firewall), Chrome sends it to Google and an Android package is created that is unique to you. It contains a unique and random identifier that is not tied to your identity.

Chrome may also download and run a binary executable (e.g., as part of the software update or to improve Safe Browsing protection). These executables are cryptographically signed and verified before execution. Chrome may download further static resources like dictionaries on demand to reduce the size of the installer.

On Windows and OS X versions of Chrome, the recovery component tries to repair Google Update when it's broken. After the relevant binary is executed, Google Update uploads statistics on the actions that were performed. These statistics contain no personally identifiable information.

Network time

On desktop platforms, Chrome uses network time to verify SSL certificates, which are valid only for a specified time. At random intervals or when Chrome encounters an expired SSL certificate, Chrome may send requests to Google to obtain the time from a trusted source. These requests are more frequent if Chrome believes the system clock is inaccurate. These requests contain no cookies and are not logged on the server.

Counting installations

In order to measure the success rate of Google Chrome downloads and installations of the Windows version of Google Chrome, a randomly-generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. A new token is generated for every install. It is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

For Chrome to know how many active installations it has, the mobile version of Chrome sends a ping to Google with a salted hash of a device identifier on an ongoing basis. The desktop version of Chrome does not send any stable identifier to count active installations. Instead an anonymous message to Google with a timestamp of the last ping is used to infer number of active installations.

Measuring effectiveness of a promotion

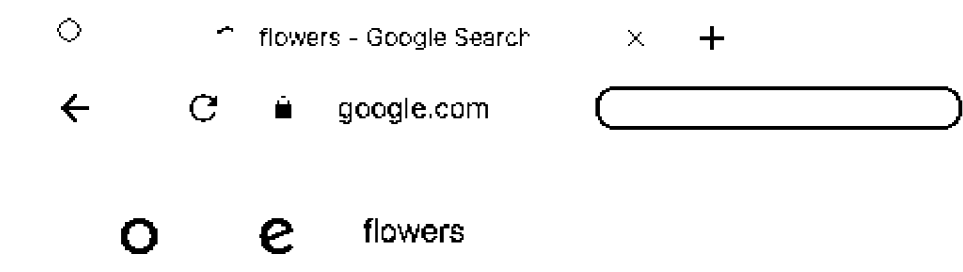
Chrome utilizes two measurements to understand how effective a promotional campaign has been: how many Chrome installations are acquired through a promotional campaign, and how much Chrome usage and traffic to Google is driven by a campaign.

To measure installations or reactivations of Chrome through a campaign, Chrome will send a token or an identifier unique to your device to Google at the first launch of Chrome, as well as the first search using Google. On desktop versions of Chrome, a token unique to your device is generated. The same token will be sent if Chrome is later reinstalled at first launch and at first use of the Omnibox after reinstallation or reactivation. Rather than storing the token on the computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner. On iOS, Chrome uses the IDFA for counting installations acquired by a campaign, and it can be reset in iOS settings.

To measure searches and Chrome usage driven by a particular campaign, Chrome inserts a promotional tag, not unique to you or your device, in the searches you perform on Google. This non-unique tag contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. For desktop versions of Chrome, Chrome generates a promotional tag, if the promotional installation token described in the previous paragraph indicates that Chrome has been installed or reactivated by a campaign on a device which has not been associated with any campaign yet. For Chrome on Mobile, a promotional tag is always sent regardless of the source of installations.

The promotional tag is generated using a software library called "RLZ" and looks similar to "1T4ADBR_enUS236US239". The RLZ library was fully open-sourced in June 2010. For more information, please see the In the Open, for RLZ post on the Chromium blog and the article "How To Read An RLZ String". On Android, this promotional tag can also be a readable string like "android-hms-tmobile-us" instead of an RLZ string, and is not unique to either you or your device.

This non-unique promotional tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to measure the searches and Chrome usage driven by a particular promotion.

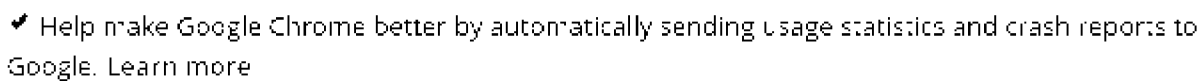


If usage statistics and crash reports are enabled, the RLZ string is sent along with the report. This allows us to improve Chrome based on variations that are limited to specific geographic regions.

For the desktop version of Chrome, you can opt-out of sending this data to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome. To opt-out of sending the RLZ string in Chrome OS, press Ctrl + Alt + T to open the crosh shell, type rlz disable followed by the enter key, and then reboot your device.

Usage statistics and crash reports

Chrome has a feature to automatically send usage statistics and crash reports to Google in order to help improve Chrome’s feature set and stability.



Usage statistics contain information such as system information, preferences, user interface feature usage, responsiveness, performance, and memory usage. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs, actions taken by the user before the crash, and/or personal information depending on what was happening at the time of the crash. This feature is enabled by default for Chrome installations of version 54 or later. You can control the feature in the "Sync and Google services" section of Chrome's settings.

When this feature is enabled, Google Chrome stores a randomly generated unique token on your device, which is sent to Google along with your usage statistics and crash reports. The token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics. This token is deleted when the feature is disabled and a new token is regenerated when the feature is enabled again.

By default, the usage statistics do not include any personal information. However, if you're signed in to Chrome and have enabled Chrome sync, Chrome may combine your declared age and gender from your Google account with our statistics to help us build products better suited for your demographics. This demographic data is not included in crash reports.

Along with usage statistics and crash reports, Chrome also reports anonymous, randomized data that is constructed in a manner which is not linked to the unique token, and which ensures that no information can be inferred about any particular user's activity. This data collection mechanism is summarized on the [Google research blog](#), and full technical details have been published in a [technical report](#) and presented at the 2014 ACM Computer and Communications Security conference.

Chrome will also anonymously report to Google if requests to websites operated by Google fail or succeed in order to detect and fix problems quickly.

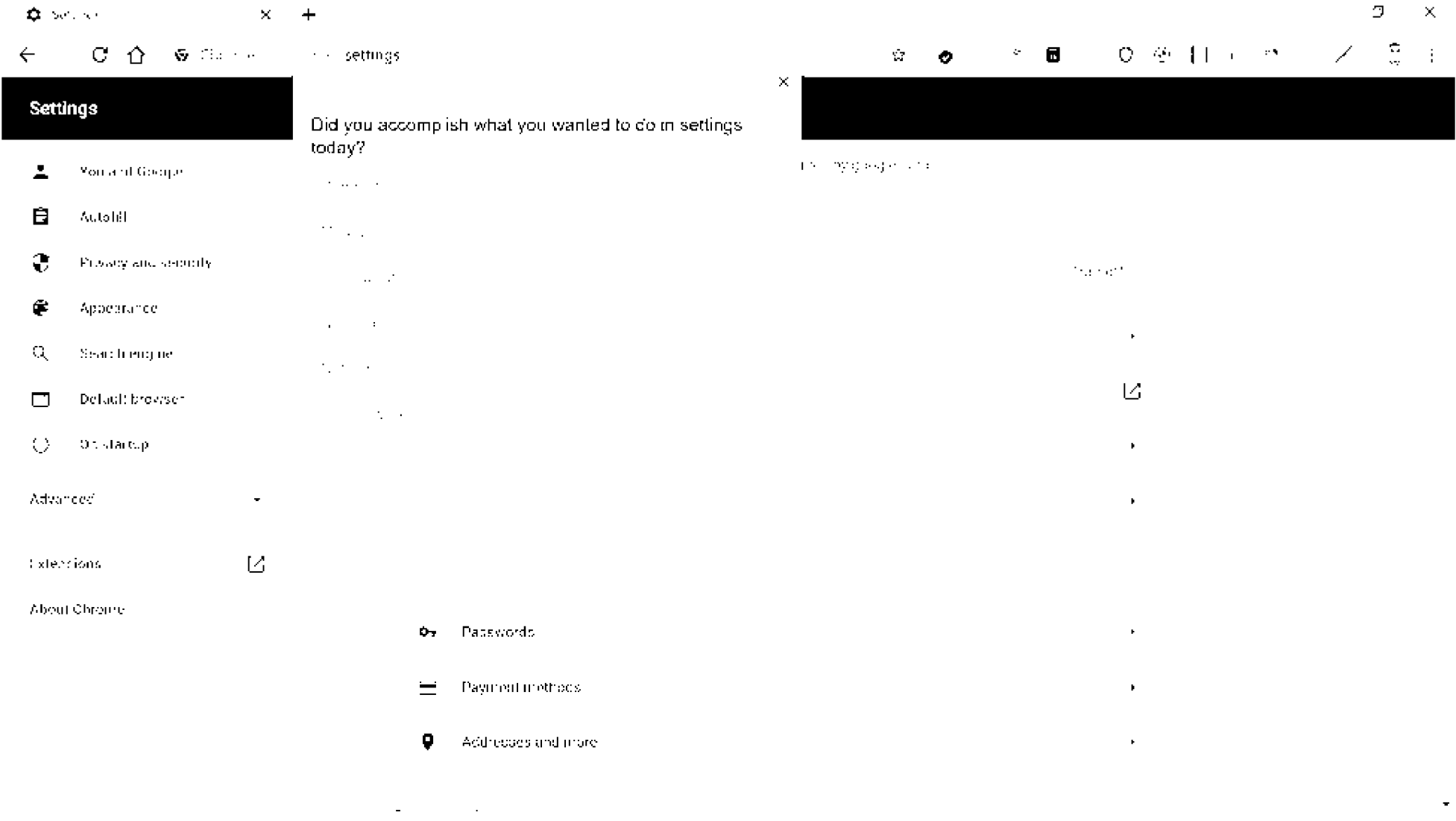
If you have also turned on “Make searches and browsing better (Sends URLs of pages you visit to Google)” in the “Sync and Google services” section of Chrome’s settings, Chrome usage statistics include information about the web pages you visit and your usage of them. The information will also include the URLs and statistics related to downloaded files. If you sync extensions, these statistics will also include information about the extensions that have been installed from Chrome Web Store. The URLs and statistics are sent along with a unique device identifier that can be reset by turning off “Make searches and browsing better” in the “Sync and Google services” section of Chrome’s settings or by turning off usage statistics and crash reports. The usage statistics are not tied to your Google account. Google only stores usage statistics associated with published extensions, and URLs that are known by Google’s web crawlers. We use this information to improve our products and services, for example, by identifying web pages which load slowly; this gives us insight into how to best improve overall Chrome performance. We also make some statistics available externally, through efforts like the [Chrome User Experience Report](#). Externally published reports are conducted in highly aggregated manner to not reveal individual user's identity.

On iOS, if you are syncing your browsing history without a sync passphrase, Chrome reports usage for certain URLs that other Google apps could open. For example, when you tap on an email address, Chrome presents a dialog that allows you to choose between opening with Google Gmail or other mail apps installed on your device. The usage information also includes which apps were presented to you, which one was selected, and if a Google app was installed. Chrome does not log the actual URL tapped. If you are signed in, this usage is tied to your Google account. If you are signed out, the information is sent to Google with a unique device identifier that can be regenerated by resetting the Google Usage ID found in Chrome settings. The raw reports are deleted within 60 days, after which only the aggregated statistics remain.

In Chrome on Android and Desktop, when you have "send usage statistics" enabled, you may be randomly selected to participate in surveys to evaluate consumer satisfaction with Chrome features. If you are selected, Chrome requests a survey from Google for you. If a survey is available, Chrome then asks you to answer the survey and submit responses to Google.

The survey also records basic metrics about your actions, such as time spent looking at the survey and elements that the user clicked. These metrics are sent to Google even if you do not fully complete the survey.

Google uses strategies to ensure that surveys are spread evenly across users and not repeatedly served to a single user. On Android, Chrome stores a randomly generated unique token on the device. On Desktop, Chrome uses a cookie to connect with the server. This token or cookie is used solely for the survey requests and does not contain any personal information. If you disable sending usage statistics, the token or cookie will be cleared.



Suggestions for spelling errors

Desktop versions of Chrome can provide smarter spell-checking by sending text you type into the browser to Google's servers, allowing you to apply the same spell-checking technology that's used by Google products like Docs. If this feature is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser's default language. Google returns a list of suggested spellings that are displayed in the context menu. Cookies are not sent along with these requests. Requests are logged temporarily and anonymously for debugging and quality improvement purposes.

This feature is disabled by default; to turn it on, click "Ask Google for suggestions" in the context menu that appears when you right-click on a misspelled word. You can also turn this feature on or off with the "Enhanced spell check" checkbox in the "Sync and Google services" section of Chrome settings. When the feature is turned off, spelling suggestions are generated locally without sending data to Google's servers.

Mobile versions of Chrome rely on the operating system to provide spell-checking.

Translate

Google Chrome's built-in translation feature helps you read more of the Web, regardless of the language of the web page. The feature is enabled by default.



Translation can be disabled at any time in Chrome's settings.

Language *detection* is done entirely using a client-side library, and does not involve any Google servers. For *translation*, the contents of a web page are only sent to Google if you decide to have it translated. You can do that on an individual basis on each page that shows a translation option or for all pages in a specific

language by choosing “Always translate” in the Translate UI. Additionally, you can do so by clicking on a translated search result on the Google Search Results Page.

If you do choose to translate a web page, the text of that page is sent to [Google Translate](#) for translation. Your cookies are not sent along with that request and the request is sent over SSL. This communication with Google's translation service is covered by the [Google privacy policy](#).

If you’ve chosen to sync your Chrome history, statistics about the languages of pages you visit and about your interactions with the translation feature will be sent to Google to improve Chrome’s understanding of the languages you speak and when Chrome should offer to translate text for you.

Image Descriptions for screen reader users

Chrome can provide automatic descriptions for users who are visually impaired by sending the contents of images on pages you visit to Google's servers. This feature is only enabled when Chrome detects that the user has a screen reader running and if the user explicitly enables it in the page context menu. Cookies are not sent along with these requests. Chrome fetches the list of supported languages from Google's servers and then requests descriptions in the most appropriate language given the current web page and the user's language preferences. Requests are not logged.

Sign In to Chrome and sync

You have the option to use the Chrome browser while signed in to your Google Account, with or without [sync](#) enabled.

On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. If you are signed in to Chrome, Chrome may offer to save your payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can [turn off Chrome sign-in](#).

When you’re signed-in and have enabled sync with your Google Account, your personal browsing data information is saved in your Google Account so you may access it when you sign in and sync to Chrome on other computers and devices. Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions, addresses, phone numbers, payment methods, and more. In advanced sync settings, you can choose which types of data to synchronize with this device. By default, all syncable data types are enabled. You can turn sync on or off in the “You and Google” section of Chrome settings.

If you have turned on sync and signed out of the account you are syncing to, sync will pause sending all syncable data to Google until you sign back in with the same account. Some sync data types (such as bookmarks and passwords) that are saved locally while sync is paused will automatically be synced to your account after you sign back in with the same account.

On mobile versions of Chrome, you can sign into or sign out of Chrome from Chrome settings. Signing into Chrome will also turn on sync. This can be done for any account that has already been added to the mobile device without authenticating again.

On both desktop and mobile, signing into Chrome keeps you signed into Google web services until you sign out of Chrome. On mobile, signing into Chrome will keep you signed in with all Google Accounts that have been added to the device. On desktop, it will keep you signed in with all Google Accounts that you added from a Google web service, unless you have set “Clear cookies and site data when you quit Chrome” in your [cookie settings](#).

On Android and desktop, Chrome signals to Google web services that you are signed into Chrome by attaching an X-Chrome-Connected and/or C-Chrome-ID-Consistency-Request header to any HTTPS requests to Google-owned domains. On iOS, the CHROME_CONNECTED cookie is used instead. This allows those Google web services to update their UI accordingly. If you are using a managed device, your system admin may disable the sign in feature or require that data be deleted when you disconnect your account.

Users can share phone numbers and text between their devices (mobile or desktop) when they are signed-in to Chrome. The transferred data is encrypted during transit and Google cannot read or store the content. To let users select the device to share with, Chrome collects the following information about devices on which a user is signed-in and stores that in the user's Google account: device manufacturer, model number, Chrome version, OS, and device type.

Google uses your personal synchronized data to provide you a consistent browsing experience across your devices, and to customize features in Chrome. You can manage your synchronized history by going to chrome://history in your Chrome browser. If “Include history from Chrome and other apps in your Web & App Activity” is checked on the [Web & App Activity](#) controls page, Google also uses your synchronized browsing data to provide personalized Google products and services to you. You can change your preference any time, and manage individual [activities associated with your Google account](#).

The paragraph above describes the use of your personal browsing history. Google also uses aggregated and anonymized synchronized browsing data to improve other Google products and services. For example, we use this information to improve Google Search by helping to detect mobile friendly pages, pages which have stopped serving content, and downloads of malware.

Case 4:20-cv-03664-YGR Document 666-13 Filed 08/05/22 Page 51 of 83

If you would like to use Google's cloud to store and sync your Chrome data without allowing any personalized and aggregated use by Google as described in the previous paragraphs, you can choose to encrypt all of your synced data with a [sync passphrase](#). If you choose this option, it's important to note that Google won't have access to the sync passphrase you set; we won't be able to help you recover data if you forget the passphrase. Regardless of how you choose to encrypt your data, all data is always sent over secure SSL connections to Google's servers.

Google will store the metadata about the days on which sync was running to improve other Google products and services.

If you're signed into Chrome and are syncing passwords and/or other types of login credentials without a sync passphrase, these credentials are stored in your Google Account. Chrome may help you sign in with credentials you've saved in Android apps on websites that are associated with the respective apps. Likewise, credentials you've saved for websites can be used to help you sign into related Android apps. You can view the credentials you've saved in Chrome and Android by visiting [passwords.google.com](#) in any browser. If you've saved credentials for Android applications, Chrome periodically sends a cookieless request to Google to get an updated list of websites that are associated with those applications. To stop websites and Android apps from automatically signing in using credentials you previously saved, you can turn off Auto Sign-In on [passwords.google.com](#) or in Chrome settings under "Autofill > Passwords". For more details see [this article](#).

To make the history page easier to use, Chrome displays favicons of visited URLs. For Chrome browsing history from your other devices, these favicons are fetched from Google servers via cookieless requests that only contain the given URL and device display DPI. Favicons are not fetched for users with sync passphrase.

On the iOS version of Chrome, if you sync your browsing history without a sync passphrase and your browser's usage statistics and crash reports setting is also enabled, your usage statistics and crash reports will include statistics about the pages you visit. You can read more in the [Usage statistics and crash reports](#) section of this Whitepaper.

All data synchronized through Google's servers is subject to [Google's Privacy Policy](#). To get an overview of the Chrome data stored for your Google Account, go to the [Chrome section of Google Dashboard](#). That page also allows you to stop synchronization completely and delete all sync data from Google's servers.

Autofill and Password Management

Google Chrome has a [form autofill feature](#) that helps you fill out forms on the web more quickly. Autofill is enabled by default, but it can be turned off at any time in Chrome's settings.

If Autofill is enabled and you encounter a web page containing a form, Chrome sends some information about that form to Google. This information includes the basic structure of the form, a hash of the web page's hostname as well as form identifiers (such as field names); randomized representation of the form identifiers, and if you have turned on the "Make searches and browsing better (Sends URLs of pages you visit to Google)" setting, also a randomized representation of the web page's URL. In response, Chrome receives a prediction of each field's data type (for example, "field X is a phone number, and field Y is a country"). This information helps Chrome match up your locally stored Autofill data with the fields of the form.

If Autofill is enabled when you *submit* a form, Chrome sends Google some information about the form along with the types of data you submitted. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), the basic structure of the form, and the observed data types for the fields (i.e., field X was a phone number, field Y was a country). The values you entered into the form are not sent to Google. This information helps Chrome improve the quality of its form-filling over time.

You can manage your Autofill entries via [Chrome's settings](#), and you can edit or delete saved information at any time. Chrome will never store full credit card information (card number, cardholder name, and expiration date) without explicit confirmation. In order to prevent offering to save cards you have shown disinterest in saving, Chrome stores the last four digits of detected credit cards locally on the device. If you scan your credit card using a phone camera, the recognition is performed locally.

Chrome may help you sign in to websites with credentials you've saved to Chrome's password manager or Google Smart Lock by autofilling sign-in forms, by offering you an account picker, or by automatically signing you in. You can manage and delete your saved credentials in the "Forms and passwords" section of Chrome's settings. If you enable [password management](#), the same kind of data about forms as described above is sent to Google to interpret password forms correctly. To enable Chrome to offer password generation that meets site-specific requirements, Chrome uploads a randomized vote on a specific password characteristic to the server once a user-created password is stored. If stored credentials are used for the first time in a username field which was already filled differently by the website itself, Chrome also transmits a short one-byte hash of the prefilled value. This allows Google to classify if the website uses a static placeholder in the username field which can be safely overwritten without deleting valuable user-specific data. Google cannot reconstruct the value from this hash.

When you sign in to a site, Chrome can give you a [warning](#) if the username/password have been exposed as a result of a data breach on some website or app. The feature is available on all platforms but only to the users signed in with a Google account. On Android the feature is only available if sync is also enabled, due to the way the accounts are managed by the OS. Being signed in to a Google account is a technical requirement that prevents abuse of the API. When you sign in to a website, Chrome will send a hashed copy of your username and password to Google encrypted with a secret key only known to Chrome. [No one, including Google, is able to derive your username or password from this encrypted copy](#). From the response, Chrome can tell if the submitted username and password

appear in the database of leaked credentials. The final resolution is done locally; Google doesn't know whether or not the credential is present in the database. [Case 4:20-cv-03664-YGR Document 666-13 Filed 08/05/22 Page 52 of 83](#)

The feature can be disabled in settings under Sync and Google services. On desktop and Android versions of Chrome, this feature is not available if Safe Browsing is turned off.

Using the same secure method described above, you can check all the saved passwords against the public data breaches in the “Passwords” section of Chrome’s settings. Once you’ve run a password check, Chrome will show a list of breached passwords. If a password in this list is outdated, you can manually edit it to store the current version. If you choose to edit, the new username/password pair will be checked automatically but only if the feature described above is not disabled.

Also, if you choose, you can bring your Autofill data with you to all your Chrome-enabled devices by [syncing it](#) as part of your browser settings (see the “Sign In to Chrome” section of this document). If you choose to sync Autofill information, field values are sent as described in “Sign In to Chrome”; otherwise, field values are not sent.

Payments

When you’re signed into Chrome with your Google Account, Chrome may offer to save payment cards and related billing addresses into payment data under the same Google Account, and include cards from your account among the autofill suggestions on payment web forms. If you're not signed in, Chrome offers to save your credit cards locally. If the card is not stored locally, you will be prompted for your CVV code or device authentication, such as Touch ID or Windows Hello, each time you use the card. In some versions of Chrome, it is possible to store a card to Google Payments and locally in Chrome at the same time, in which case Chrome will not ask for a CVV or device authentication confirmation. If you have cards stored in this way, their local copies will persist until you sign out of your Google account, at which point the local copy will be deleted from your device. If you choose not to store the card locally, you will be prompted for your CVV code or device authentication each time you use the card. You can [opt out of using device authentication](#) in the Payment methods section of Chrome settings. If you use a card from Google Payments, Chrome will collect information about your computer and share it with Google Payments to prevent fraudulent use of your card.

To delete credit card information saved in Chrome, follow the “Add and edit credit cards” steps in [the Autofill article](#). When you delete a credit card that's also saved in your Google Payments account, you will be redirected to Google Payments to complete the deletion. After your card has been deleted from your Google Payments account, Chrome will automatically remove that card from your Autofill suggestions.

To save a card locally on the device only, while still being signed in to Chrome with a Google Account, you can add a card from the “Add” button in the “Payment methods” section in Chrome settings. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can [turn off Chrome sign-in](#). If you have sync turned on, you can disable syncing payment methods and addresses to Google Pay under “Sync” in Chrome settings. You can also turn the Payments Autofill feature off altogether in [settings](#).

Chrome also supports the [PaymentRequest API](#) by allowing you to pay for purchases with credit cards from Autofill, Google Payments, and other payment apps already installed on your device. Google Payments and other payment apps are only available on Android devices. PaymentRequest allows the merchant to request the following information: full name, shipping address, billing address, phone number, email, credit card number, credit card expiration, CVV, and Google Payments credentials. Information is not shared with the merchant until you agree.

Geolocation

Google Chrome supports the [Geolocation API](#), which provides access to fine-grained user location information with your consent.

By default, Chrome will request your permission when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.

Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In Chrome’s settings, by clicking “Site Settings” and scrolling to the “Location” section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

In the Android version of Chrome, your default search engine automatically receives your location when you conduct a search. On the iOS version of Chrome, by default your location is sent to Google if you conduct a search from the omnibox. Read more about how your default search engine handles geolocation and how to manage your settings in the [Omnibox](#) section of the whitepaper.

If you do choose to share your location with a web site, Chrome will send local network information to Google (also used by other browsers such as Mozilla Firefox) in order to estimate your location. This local network information can include data about nearby Wi-Fi access points or cellular signal sites/towers (even if you’re not using them), and your computer’s IP address. The requests are logged, and aggregated and anonymized before being used to operate, support, and improve the overall quality of Google Chrome and Google Location Services.

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see [“Practical Privacy Concerns in a Real World Browser”](#) written by two Google Chrome team members.

Speech to text

Chrome supports the [Web Speech API](#), a mechanism for converting speech to text on a web page. It uses Google's servers to perform the conversion. Using the feature sends an audio recording to Google (audio data is not sent directly to the page itself), along with the domain of the website using the API, your default browser language and the language settings of the website. Cookies are not sent along with these requests.

Google Assistant on Chrome OS devices

The Google Assistant is integrated into some models of Chrome OS devices. If you opt in to the feature, Chrome OS listens for you to say "Ok Google" and sends the audio of the next thing you say, plus a few seconds before, to Google. Detection of the phrase "Ok Google" is performed locally on your computer, and the audio is only sent to Google after it detects "Ok Google". You can enable or disable this feature in Google Assistant Settings.

Enabling this feature in Chrome Settings will cause Chrome to listen whenever the screen is unlocked. On Chrome OS devices with a local audio processor, the device also listens when the device is asleep. On these devices, The Google Assistant feature only works if [Voice & Audio Activity](#) is enabled for your Google account. Chrome will prompt you to enable [Voice & Audio Activity](#) for the associated Google account if it is disabled.

Once the audio has been converted to text, a search with that text is submitted to Google. If you have used the “Ok Google” search before on a device but turned off Voice & Audio Activity later, your device is still capable of processing your voice and sending the audio to Google but the voice is deleted shortly thereafter.

You can determine your Chrome OS device’s behavior by examining the text in the "Search and Assistant" section of settings.

Google Assistant on Android devices

You can quickly complete tasks on the web using the Google Assistant in Chrome on certain Android devices . If you opt-in to this feature, you can speak to the Google Assistant and ask it to search websites. It also can fill out forms on your behalf, or speed up the checkout experience.

For example, if you issue a command to the Google Assistant e.g. “search Wikipedia for Henry VIII”, the Google Assistant in Chrome will respond by opening Chrome to Wikipedia, sending the query as a text string to Google Assistant in Chrome, and searching for “Henry VIII” on the Wikipedia page.

As another example, if you ask the Google Assistant to help you purchase tickets for an upcoming movie, then the address of the website you are viewing, your credit card information, and your email address will be shared with Google to complete the transaction and make it possible for you to receive the purchase receipt and movie ticket.

If you opt-in to this feature, the Google Assistant in Chrome will send data to Google in order to complete the command you issued. When the command is issued, the Google Assistant in Chrome shares back to Google the website’s URL to validate that the webpage is allowed to be automated by Google Assistant in Chrome and to receive the instructions on how to complete the task (e.g. on how to fill out a form).

At the time the command you issued is executed, additional information can be shared. Depending on the command you issued, the information shared with Google can include the address of the website you are viewing, your email address, your name, your delivery and billing address, your credit card information, and possibly the username you use to log into the website. This information is not stored by Google — rather, this information is passed on to the third party website to complete the command you issued to the Google Assistant. Additionally, information about your system is collected in order to improve the product and to debug issues.

Some Google Assistant features are not available on Incognito tabs. You can turn off the ability to use the Google Assistant in Chrome on your Android device by toggling the “Google Assistant for Chrome” option in Chrome’s settings.

Google Cloud Print

The [Google Cloud Print](#) feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google’s servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google’s servers.

A print job will be downloaded by either a Chrome browser (“Connector”) or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP’s ePrint, for example).

The print job is deleted from Google’s servers when any of three criteria is met:

- You delete the print job
- The job has been printed and marked as printed by the printer/connector
- The job has been queued on Google’s servers for 30 days

You can manage your printers and print jobs on the [Google Cloud Print website](#).

SSL certificate reporting

Chrome stores locally a list of expected SSL certificate information for a variety of high-value websites, in an effort to [prevent man-in-the-middle attacks](#). For Google websites and other websites that choose to opt in, Chrome will report a possible attack or misconfiguration. If the certificate provided by the web server doesn’t match the expected signature, Chrome reports information about the SSL certificate chain to Google or to a report collection endpoint of the website’s choosing. Chrome sends these reports only for certificate chains that use a [public root of trust](#).

You can enable this feature by opting in to report data relevant to security, as described in the [Safe Browsing section](#). While you are opted in, two kinds of reports may be sent to Google’s security team. Each time you see an SSL error page, a report will be sent containising the SSL certificate chain, the server’s hostname, the local time, and relevant details about the validation error and SSL error page type. Additionally, each time a mismatch between different certificate verifiers is detected, a report will be sent containing the certificate chain and the verification result.

Because Chrome sends these reports for all certificate chains, even those that chain to a private root of trust, these chains can contain personally identifiable information. You can opt out anytime by unchecking the box “Help Improve Chrome security” in “Privacy and security > Security”.

The SSL certificate reporting feature is not available on Chrome iOS.

Installed Applications and Extensions

Users can install external apps and extensions for the desktop versions of Chrome to add features to or customize their Chrome browsers. Installing an application or extension from the Chrome Web Store directly or via an [inline installation](#) flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you’re logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google Update.

As they’re more deeply integrated into Chrome, applications and extensions that you choose to install can request access to additional capabilities, enabling functionality that doesn’t make sense on the web at large: background notifications or raw socket access, for instance. These additional permissions may change the way your data is collected and shared, as extensions and applications might have access to data regarding the websites you visit, and might be capable of monitoring or modifying your interactions with the web. When installing an application or extension, Chrome may first warn you about [certain capabilities](#). Please do take the time to read and evaluate this warning before proceeding with the installation. Note also that interactions with and data collected by these third-party applications and extensions are governed by their own privacy policies, not Google’s privacy policy.

Push messaging

Case 4:20-cv-03664-YGR Document 666-13 Filed 08/05/22 Page 55 of 83

Your device may receive push messages from the backend servers of apps and extensions installed in Chrome, websites that you grant the “notification” permission to, and your default search engine. Disabling push messages from your default search engine is done in the same way as disabling push messages from any site, by visiting the “Notifications” section of “Site settings”.

Push message data is sent over a secure channel from the developer through Google's infrastructure to Chrome on your device, which can wake up apps, extensions, and websites (including your default search engine) to deliver the message. The developer may end-to-end encrypt the message data, or may send it in a form such that Google servers process it as plain text. Google servers retain up to 4 weeks’ worth of messages to ensure delivery to users even if their devices are offline at the time of the initial pushing.

If the notification permission is set to “granted” for any website (including the default search engine), or you have an app or extension installed that uses push messaging, then Chrome provides the app’s, extension’s, or website’s server with one or more registration tokens that can be used to send messages to the entity (app, extension, or website). Websites you visit in Incognito mode are not allowed to send you push messages and therefore cannot get a registration token.

When you uninstall an app or extension, revoke the notification permission for a website, or clear cookies for a permitted website, its registration token is revoked and will not be reused, even if the same app or extension is re-installed or the same website is re-visited. Registration tokens used by Chrome components such as Sync are revoked once they are no longer in use (for example, when the user disables Sync). When a registration token is revoked, the associated entity on your device stops receiving messages sent from its developer’s server.

The registration tokens that are passed to entities contain an encrypted device ID, which is used for routing the messages. Google can decrypt the device ID, but other entities cannot, and the encryption is designed so that two registration tokens for the same device ID cannot be correlated. On desktop versions of Chrome, the device ID is reset when the Chrome profile is removed, or when neither Chrome Sync nor any of the entities requires it for push messaging. On Android, the lifetime of the device ID is governed by the operating system and is independent of Chrome. Any messages routed to registration tokens containing a revoked device ID will not be delivered.

Chrome custom tabs

On Android devices, an app developer may use a Custom Tab to show web content when you click on a URL from their app. A Custom Tab may look different from a regular Chrome tab, for example it may have app-specified visual style, and the absence of an editable URL bar. Despite the different visual style a Custom Tab may have, the data sent and received in the Custom Tab, such as cookies, saved passwords and browsing history function the same way they do in a normal Chrome tab. The Custom Tab is an app-customized view using the same underlying user profile.

With Chrome Custom Tabs, an Android app developer may also specify custom actions in the Chrome toolbar and overflow menu that are relevant to their app, for example,"share", “save page”, “copy URL”. If you tap on such a button, the address of the current website is shared with the application.

An application can request Chrome to pre-render a given URL in the background. This allows Chrome to show you a pre-loaded site instantly when you open it from the app. At the same time it allows an application to set cookies in your browser in the background. To disable pre-rendering, you can uncheck "Preload pages for faster browsing and searching" in the “Privacy and security > Cookies” section of Chrome’s settings.

Trusted Web Activities are a form of Chrome Custom Tab where the top bar is not present, allowing web browsing with no browser UI but with access to the cookie jar. They can only be used to view web content on an origin that the client app can prove that it owns using Digital Asset Links. If the user navigates off this origin the the top bar reappears.

When the client app is uninstalled or has its data cleared through Android Settings, Chrome will allow the user to clear data for the linked origin.

Continue where you left off

If you have selected the option to “Continue where you left off” in settings on desktop versions of Chrome, when you open Chrome, it attempts to bring you right back to the way things were when the browser was closed. Chrome reloads the tabs you had open and persists session information to get you up and running as quickly as possible. This feature effectively extends a browsing session across restarts. In this mode, session cookies are no longer deleted when the browser closes; instead, they remain available on restart to keep you logged into your favorite sites.

On desktop versions of Chrome, this feature can be enabled or disabled in Chrome settings. On Chrome OS, it is enabled by default.

On OS X, when you restart your device, a checkbox in the OS confirmation dialog asks you whether you want to re-open applications and windows after restart. If you check this box, Chrome restores tabs and windows, as well as the session cookies, even if you have disabled "Continue where you left off" on Chrome.

On mobile versions of Chrome, this feature is always enabled without a setting.

Chrome is constantly evolving to better meet the needs of users and the web. To ensure new features are providing the best experience and working correctly, they may be enabled for a subset of users before they are fully launched. For example, if we improve how page loading works in Chrome, we may try it out for 1% of users to ensure that it doesn't crash or run slower before launching to everyone. This is done through a system called "Chrome Variations" - also known as "field trials".

A given Chrome installation may be participating in a number of different variations (for different features) at the same time. These fall into two categories:

1. Low entropy variations, which are randomized based on a number from 0 to 7999 (13 bits) that's randomly generated by each Chrome installation on the first run.
2. High entropy variations, which are randomized using the usage statistics token for Chrome installations that have usage statistics reporting enabled.

Other factors may additionally inform the variations assigned to a Chrome installation, such as country (determined by your IP address), operating system, Chrome version and other parameters.

Usage statistics and crash reports are tagged with all variations a client participates in, including both low entropy and high entropy variations. These reports, which also contain a pseudonymous client identifier, can be disabled in Chrome settings.

Additionally, a subset of low entropy variations are included in network requests sent to Google. The combined state of these variations is non-identifying, since it is based on a 13-bit low entropy value (see above). These are transmitted using the "X-Client-Data" HTTP header, which contains a list of active variations. On Android, this header may include a limited set of external server-side experiments, which may affect the Chrome installation. This header is used to evaluate the effect on Google servers - for example, a networking change may affect YouTube video load speed or an Omnibox ranking update may result in more helpful Google Search results.

On Android Chrome, in certain cases these low entropy variations may also be sent to Google apps when cross-app communication occurs to support a Chrome feature; for example, when searching with [Google Lens](#). This information is used to better understand how Chrome experiments affect that Google feature: for example, Chrome memory usage change could affect how long it takes an action in the Google app to complete.

You can reset the variations used by your Chrome installation by starting it with the "--reset-variation-state" command line flag.

Do Not Track

If you enable the "Do Not Track" preference in Chrome's settings, Chrome will send a DNT:1 HTTP header with your outgoing HTTP, HTTPS and SPDY browsing traffic (Chrome cannot, however, guarantee that NPAPI plugins also send the header.) The header will not be sent with system traffic such as the geolocation, metrics or device management services.

The effect of Do Not Track depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example, to improve security; to provide content, services, ads and recommendations on their websites; and to generate reporting statistics.

Chrome on iOS now uses WKWebView to provide a more stable and faster browser. As a result of this move, the Do Not Track preference is no longer available due to iOS constraints. If Apple makes changes to allow this feature, Chrome will make Do Not Track available again in iOS.

Plugins

Chrome ships with an Adobe Flash Player implementation that is based on the Pepper API. Flash and other Pepper-based plugins may ask you for "Access to your computer". If you grant this permission, the plugin is granted unsandboxed access. This allows content providers to offer you access to DRM protected content like videos or music but may have security and privacy implications, so consider carefully whether you trust a plugin or website with this privilege.

Media licenses

Some websites encrypt media to protect against unauthorized access and copying. When users play media from these sites, they typically log into the site, which authenticates the user, and then digital rights management negotiates a key exchange for the decryption and playback of the media.

For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. The implementation of that API is tightly coupled with the browser to protect user privacy and security, through Content Decryption Modules (CDM), which are provided by digital rights management solutions such as Google Widevine or Microsoft PlayReady.

When a user asks Chrome to play encrypted HTML5 media (for example, watching a movie on Google Play Movies), Chrome will generate a request for a license to decrypt that media. This license request contains an automatically generated request ID, which is created by the Content Decryption Module, as well as proof that the CDM is legitimate. After generation, the license request is typically sent to a license server managed by either the content website or Google. Neither the license request, the proof, nor the request ID include any personally identifying information. After being sent, the license request is not stored locally on the user's device.

As part of the license request, Chrome also generates a unique session ID which does not contain personally identifying information. This session ID is sent to the license server, and when the server returns a license the session ID is used to decrypt the media. The session ID may be stored locally even after the site has been closed. The license may also be stored locally for offline consumption of protected content. Session ID and licenses may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

When returning a license, the site license server may include a client ID, generated by the site. This client ID is unique to the user and the site, it is not shared between sites. If provided, the client ID is stored locally and included by Chrome in subsequent license requests to that site. The client ID may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

On some platforms, the website may additionally request verification that the device is eligible to play specific types of protected content. On Chrome OS, this is known as [Verified Access](#). In this case, Google creates a certificate using a unique hardware identifier for the device. This hardware ID identifies the device, but does not identify the user. If the user agrees, Google receives the hardware ID and generates a certificate verifying the device for the requested site. The certificate does not include the hardware ID or any other information that could permanently identify the device. Certificates are stored locally similar to other cached browsing data, and may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected. On Android, this is called [Provisioning](#). See “[MediaDrm Provisioning](#)” for more details.

Some sites use Flash instead of HTML5. If a website you visit chooses to use Adobe Flash Access DRM protection, Chrome for Windows and Chrome OS will give Adobe Flash access to a device identifier. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with “Cookies and other site data” selected.

In order to give you access to licensed music, the [Google Play Music app](#) can retrieve a device identifier that is derived from your hard drive partitions or, on a Chrome OS or Linux installation, from a unique file on your disk. This identifier can be reset by reinstalling your operating system.

MediaDrm provisioning

Chrome on Android uses [Android MediaDrm](#) to play protected content. As on ChromeOS, the website may request verification that the device is eligible to do so. This is achieved by MediaDrm provisioning. A provisioning request is sent to Google, which generates a certificate that will be stored on the device and sent to the site whenever you play protected content. The information in the provisioning request and in the certificate vary depending on the Android version. In all cases, the information can be used to identify the device, but never the user.

On Android K and L, the device only needs to be provisioned once and the certificate is shared by all applications running on the device. The request contains a hardware ID, and the certificate contains a stable device ID, both of which could be used to permanently identify the device.

On Android M or later, MediaDrm supports per-origin provisioning. Chrome randomly generates an origin ID for each website to be provisioned. Even though the request still contains a hardware ID, the certificate is different for each website, so that different websites cannot cross-reference the same device.

On Android O or later on some devices, provisioning can be scoped to a single application. The request will contain a hardware ID, but the certificate will be different for each application, in addition to each site, so different applications cannot cross-reference the same device.

Provisioning can be controlled by the “Protected media” permission in the “Site settings” menu. On Android versions K and L, Chrome will always ask you to grant this permission before provisioning starts. On later versions of Android, this permission is granted by default. You can clear the provisioned certificates anytime using the “Cookies and other site data” option in the [Clear browsing data](#) dialog.

Chrome also performs MediaDrm pre-provisioning to support playback of protected content in cases where the provisioning server is not accessible, such as in-flight entertainment. Chrome randomly generates a list of origin IDs and provision them in advance for future use.

On Android versions with per-device provisioning, where provisioning requires a permission, Chrome does not support pre-provisioning. Playback might still work because the device could have already been provisioned by other applications.

On Android versions with per-origin provisioning, Chrome pre-provisions itself once the user attempts to play protected content. As the provisioning for the first playback already involved sending a stable hardware ID to Google, the subsequent pre-provisioning of additional origin IDs introduces no new privacy implications. If provisioning fails and there is no pre-provisioned origin ID, Chrome may ask for permission to further fallback to per-device provisioning.

Cloud policy

When you sign into a Chrome OS device, Chrome on Android, or a desktop Chrome profile with an account associated with a Google Apps domain, or if your desktop browser is enrolled in Chrome Browser Cloud Management, Chrome checks whether the domain has configured enterprise policies. If so, the Chrome OS user session, Chrome profile, or enrolled Chrome Browser is assigned a unique ID, and registered as belonging to that Google Apps domain. Any configured policies are applied. To revoke the registration, remove the Chrome OS user, sign out of Chrome on Android, remove the desktop profile, or remove the enrollment token and device token for Chrome Browser Cloud Management.

Additionally, Chrome OS devices can be enrolled to a Google Apps domain by a domain admin. This will enforce enterprise policies for the entire device, such as providing shared network configurations and restricting access to developer mode. When a Chrome OS device is enrolled to a domain, then a unique device ID is registered to the device. In order to revoke the registration, the admin will need to wipe the entire Chrome OS device.

Registered profiles and devices check for policy changes periodically (every 3 hours by default). In some cases, the server pushes policy changes to the client without waiting for Chrome's periodic check. Unregistered profiles check whether a policy has been turned on for their domain each time Chrome starts up.

The policy list contains details about the types of configurations that are available via Cloud Policy.

Lite Mode

If you enable Lite Mode, Chrome will send your traffic through Google's optimizing proxy servers. This option reduces the amount of data downloaded and speeds up your page loads. This feature was previously known as “Data Saver”.

Most of the time, only your HTTP traffic is transparently proxied, and you won't notice any changes to the page. However, if Chrome anticipates the page will load especially slowly, both HTTP and HTTPS pages will be optimized to load faster. For HTTPS origins, the transcoded pages are served from a Google-owned domain instead of being transparently proxied. Because these pages are served from a Google-owned domain instead of the original domain, Chrome will not send any origin-scoped information (e.g., cookies or data from local storage) for the original domain to Google, and Google cannot set any origin-scoped information for the original domain in Chrome. Pages loaded in Incognito are never proxied or optimized by Lite Mode.

Additionally, when you enable Lite Mode, Chrome may share the URLs and usage and performance statistics of the websites you visited with Google in order to identify the websites that load slowly and improve their performance.

Request URLs are logged, but Cookie and If-None-Match headers are stripped from the logs (and cookies are never seen in the case of HTTPS pages). Additionally, the content of proxied pages is cached but not logged. The logs are not associated with your Google Account, and the entire log entry is removed within 14 days. These logs are also governed by standard Google search logging policies.

Google uses the logged and cached data to improve both Lite Mode and Safe Browsing; for example, more effective optimizations can be uncovered by analyzing timing data for pages loaded through the proxy service, and malware can be detected more rapidly by analyzing response data in realtime.

Your IP address is forwarded to the origin HTTP server via an X-Forwarded-For header, in accordance with the HTTP standard. The Lite Mode service is a transparent proxy, *not* an anonymization service.

By default, the connection between the browser and the Lite Mode proxy is over an encrypted channel. However, a network administrator can disable the use of an encrypted channel to Lite Mode.

To further improve loading performance for Lite mode users, if you have the “Preload pages for faster browsing and searching” setting enabled, Chrome may prefetch search result links found on the Google Search page. Four mechanisms preserve user privacy for these prefetches:

- Prefetching is disabled if Chrome has a cookie for the domain.
- Passive fingerprinting surfaces such as User-Agent are bucketed or set to fixed values.
- Prefetches are tunneled through a CONNECT proxy operated by Google, and only HTTPS links are prefetched. Consequently, the TLS connection is established between Chrome and the origin so the proxy server cannot inspect the traffic, and requests to the origin come from a Google IP instead of the user's IP. Google only learns about the destination domain that will be prefetched, which Google already knows as it generated the Search results page.
- Prefetched resources and cookies set by the prefetched domain are only persisted when you click the search result and visit the prefetched domain.

Using Chrome with a kid's Google Account

Case 4:20-cv-03664-YGR Document 666-13 Filed 08/05/22 Page 59 of 83

Chrome for Android offers features to be used when signed in with a kid's Google Account and automatically signs in a kid's account if they've signed into the Android device. Chrome uses the Sync feature to sync settings configured by parents to the kid's account. You can read about how Sync data is used in the Sign in section of this Whitepaper.

The collection and use of Chrome data in association with a kid's Google Account are governed by the Google Family Link - Children's Privacy Policy.

In order for the configured settings to apply to a kid's account, Chrome does not support the following features for a kid's Google Account: signing out of Chrome, Incognito mode, and deleting browsing history from within Chrome. Browsing history can still be removed in the Chrome section of the Google Dashboard.

By default, first party cookie blocking is disabled when Chrome is signed in with a kid's account. Parents can go to chrome.google.com/manage/family to allow their kids to block first party cookies. However, blocking cookies signs kids out of Google web products such as Google Search or YouTube and therefore prevents these products from providing any features designed for kids' Google Accounts.

When Chrome is used with a kid's Google Account, information about the kid's requests to access blocked content is sent to Google and made visible to the kid's parent(s) on chrome.google.com/manage/family and in the Google Family Link app. If the kid's browsing mode is set to "Try to block mature sites", Chrome will send a request to the Google SafeSearch service for each navigation in order to block access to sites that have been classified as containing mature content.

Incognito and Guest Mode

Incognito mode in Chrome is a temporary browsing mode. It ensures that you don't leave browsing history and cookies on your computer. The browsing history and cookies are deleted only once you have closed the last incognito window. Incognito mode cannot make you invisible on the internet. Websites that you navigate to may record your visits. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Browsing as a Guest in Chrome allows you to use somebody else's computer without modifying their profile. For example, no bookmarks or passwords get stored on their computer. Note that Guest mode does not protect you for example, if the computer you are using is infected by a keylogger that records what you type.

iOS 8 and Mac OS X Yosemite Handoff Support

While browsing in a standard (i.e. non-Incognito) session, Chrome will share your current URL with iOS 8+ to support the Handoff feature that was added in OS X Yosemite. This information is only sent to Apple devices that are paired with your iOS device, and the data is encrypted in transit.

More information is available at Apple Support, Apple Developers, and in the Apple iOS Security Guide. Chrome support for this feature can be disabled in Chrome settings.

Security Key

A FIDO U2F Security Key provides a non-phishable credential which can be used to authenticate a user. This mitigates the risk of various kinds of man-in-the-middle attacks in which websites try to steal your password and use it later.

To prevent abuse, a website is required to be delivered over a secure connection (HTTPS), and to register the security key before it can be used for identification. Once a website is registered with a specific security key, that security key will provide a persistent identifier, regardless of which computer it is plugged into, or whether you're in incognito or guest mode, but you must physically interact with the security key to give a website access to an identifier (by, for example, touching it, or plugging it in).

Physical Web

The Physical Web lets you see a list of URLs being broadcast by objects in the environment around you. Google Chrome looks for Physical Web devices with Bluetooth Low Energy beacons that are broadcasting URLs using the Eddystone protocol. Bluetooth signals can be received from 90 feet away or more, depending on signal strength and the user's environment (although the range is often much shorter, due to obstacles and signal noise). If the Physical Web feature is enabled, Chrome sends detected URLs to Google's Physical Web Service (PWS) via a cookieless HTTPS request. For each URL, the PWS obtains the title of the web page, filters out unsafe results, and returns a ranking based on non-personalized signals about the quality and relevance of the web page.

The Physical Web feature is available on Chrome on iOS and Android. Users will need to turn on Bluetooth to use the feature.

If Android users have location settings enabled on both their device and in Chrome, they will receive a notification the first time they are near a beacon that will give them the option to turn on the Physical Web feature. This beacon's URL is not sent to Google's PWS unless the Physical Web feature is enabled. Users can also enable (or disable) the feature in the Privacy settings. Once a user enables the feature, Chrome scans for nearby devices for a few seconds each time the user unlocks the mobile device in use and sends them to the PWS in order to obtain more information about the beacon. The user receives a silent notification when Chrome finds a nearby URL.

On iOS devices, users can [enable](#) (or disable) the feature in the Privacy settings or by adding the Chrome widget to their Today view in the notification center. Additionally, the feature is automatically enabled for users who have location enabled on their device, granted Chrome the location permission, and have granted Google the geolocation permission. Chrome scans for nearby devices whenever it is open in the foreground. When Chrome finds nearby URLs, users will see them as omnibox suggestions. Additionally, Chrome scans for nearby devices for a few seconds when the Today widget is displayed in the notification center.

Bluetooth

Google Chrome supports the [Web Bluetooth API](#), which provides websites with access to nearby [Bluetooth Low Energy devices](#) with your consent.

Chrome does not let any page communicate with a device unless you explicitly consent. When a web page asks to pair with a device, Chrome will ask you to choose which device the web page should access, if any. Selecting a device for one page does not give other pages access to the device you have chosen, and does not allow that page to access other devices. Currently, permission for a page to communicate with a device is usually revoked when the page is reloaded, and is always revoked when Chrome is restarted.

Chrome data that Android sends to Google

The data collection and usage described in this section is handled by Android and governed by the [Google Privacy Policy](#).

If the Android Backup Service is enabled on your device, some of your Chrome preferences will be saved and stored on Google servers. For Nexus and Android One devices, it is described under “Back up your data and settings with Android Backup Service” in [this article](#). For other Android devices, you may be able to find help by looking up your device on [this page](#). When setting up a new Android device, you may request that it copies the preferences from a previously set up device. If you do so, Android may restore backed up Chrome preferences when Chrome is first installed. The new device only copies the preferences if automatic restore is enabled (see “Restore your data and settings” in [the same article](#)), Chrome was signed into an account when the backup was made, and the new Android device is signed into that same account.

Chrome’s backup data for a particular device may also be restored if you uninstall and then later re-install Chrome on that device. This will only happen if automatic restore is enabled and the device is signed into the account that Chrome was signed into when the backup was made.

Integration with Digital Wellbeing

If you opt-in to see sites you have visited and set site timers in the Digital Wellbeing app on Android, Chrome will report which websites you’ve visited and the length of time spent in each of them to the app. Sites visited in incognito mode will not be reported to the Digital Wellbeing app.

To continually improve the experience of Digital Wellbeing, the app will share with Google the websites that you set a timer on and how long you have visited them.

You can opt out of this feature in the Digital Wellbeing app or in Chrome’s privacy settings anytime.

Follow us



Chrome Family

Enterprise

Education

Dev and Partners

Stay Connected

Other Platforms

Download Chrome
Browser

Google Chrome Browser

Chromium

Google Chrome Blog

Chromebooks

Chrome Browser for
Enterprise

Devices

Chrome OS

Update Chrome

Chromecast

Web Store

Chrome Web Store

Chrome Help

Chrome Cleanup Tool

Chrome Devices

Chrome Experiments

Chrome Tips

Chrome OS

Chrome Beta

Google Cloud

Chrome Dev

Google Workspace

Chrome Canary

EXHIBIT 20

Google Chrome Privacy Whitepaper

Last modified: April 07, 2020 (Current as of Chrome 81.0.4044.69)

Omnibox | Network predictions | Search locale | New Tab page | Touch to Search | Safe Browsing protection | Unwanted software protection | Navigation errors | Offline Indicator | Google update | Network time | Counting install | Measuring promotions | Usage stats | Google Surveys | Spelling suggestions | Translate | Image Descriptions | Signing In | Autofill | Payments | Geolocation | Speech to text | Google Assistant on Chrome OS devices | Google Assistant on Android devices | Cloud Print | SSL certificate error reporting | Installed apps | Push Messaging | Chrome custom tabs | Continue where you left off | Chrome variations | Do Not Track | Plugins | Media licenses | MediaDrm provisioning | Cloud policy | Lite Mode (Chrome mobile) | Kid’s Google Account | Incognito and Guest mode | Handoff support | Security key | Physical web | Bluetooth | Data sent by Android | Integration with Digital Wellbeing |

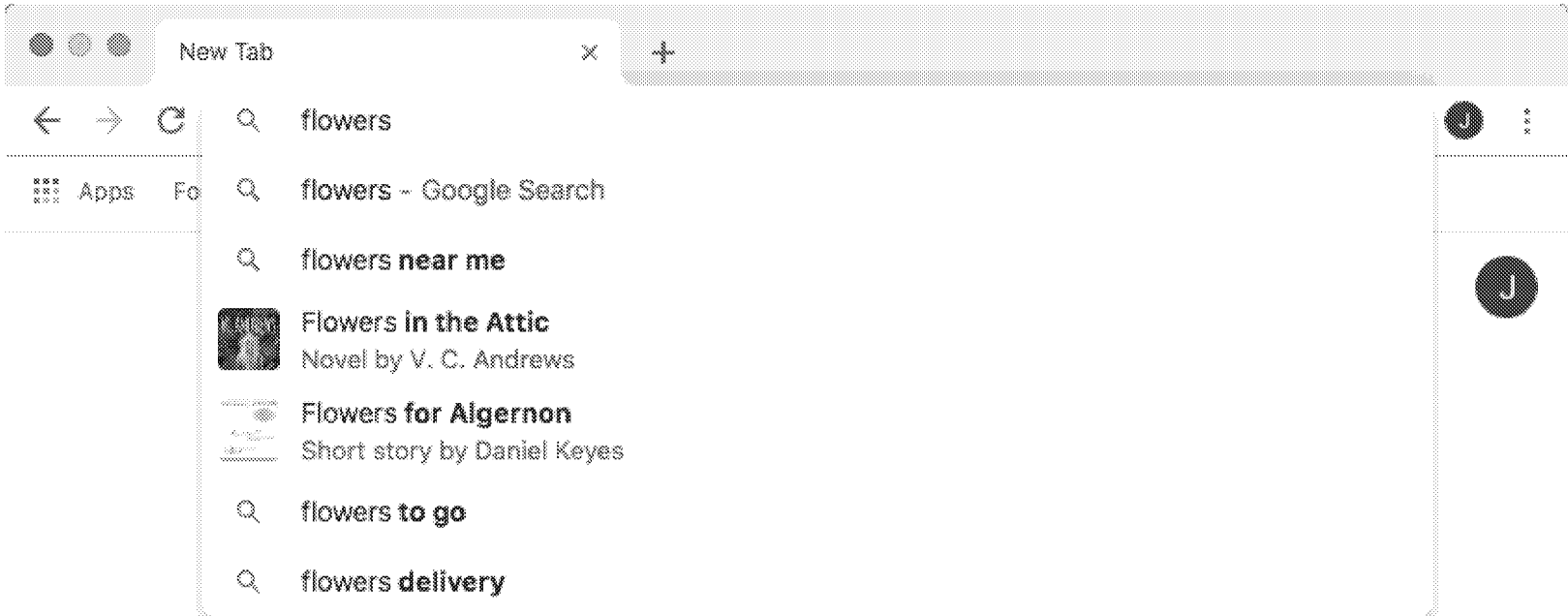
This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine). This document also describes the controls available to you regarding how your data is used by Chrome. Here we’re focusing on the desktop version of Chrome; we touch only tangentially on Chrome OS and Chrome for Mobile. This document does not cover features that are still under development, such as features in the beta, dev and canary channel and active field trials, or Android apps on Chrome OS if Play Apps are enabled.

If you have a question about Google Chrome and Privacy that this document doesn’t answer, please feel free to ask it in the [Community Forum](#). If you want to report a privacy issue, you can file it in [our public bug tracker](#). For issues that include confidential information, please use [this link](#). We’d be happy to hear from you.

Omnibox

Google Chrome uses a combined [web address and search bar](#) (we call it the “omnibox”) at the top of the browser window.

As you use the omnibox, your [default search engine](#) can suggest addresses and search queries that may be of interest to you. These suggestions make navigation and searching faster and easier, and are turned on by default. They can be turned off by unchecking "Autocomplete searches and URLs" in the “Sync and Google services” section of Chrome's settings.



When not in Incognito mode, in order to provide these suggestions, Chrome sends the text you've typed into the omnibox, along with a general categorization (e.g., "URL", "search query", or "unknown"), to your default search engine. Chrome will also send a signal to your default search engine when you focus in the omnibox, telling it to get ready to provide suggestions. That signal includes the URL of the currently displayed search engine results page. Your IP address and certain cookies are also sent to your default search engine with all requests, in order to return the results that are most relevant to you.

To provide suggestions and search results faster, Chrome may preconnect to your default search engine in the background. Chrome will not preconnect if you have either turned off “Preload pages for faster browsing and searching” in the “Privacy and security” section or "Autocomplete searches and URLs" in the “Sync and Google services” section of Chrome's settings. When Chrome preconnects, it resolves the search engine’s IP address and connects it to the search engine, exposing your IP address.

When in Incognito mode, in order to provide these suggestions, Chrome relies on an on-device model that does not communicate with your default search engine until you select a suggestion.

If Chrome determines that your typing may contain sensitive information, such as authentication credentials, local file names, or URL data that is normally

If Google is your default search engine, when you select one of the omnibox suggestions, Chrome sends your original search query, the suggestion you selected, and the position of the suggestion back to Google. This information helps improve the quality of the suggestion feature, and it's logged and anonymized in the same manner as Google web searches. Logs of these suggestion requests are retained for two weeks, after which 2% of the log data is randomly selected, anonymized, and retained in order to improve the suggestion feature.

If you've chosen to sync your Chrome history, and if Google is your default search engine, the URL of the page you're viewing is sent to Google in order to provide better, contextually relevant suggestions. URLs are sent only for HTTP pages and HTTPS pages, not other schemes such as file: and ftp:. Additionally, Chrome may present website and search query suggestions as soon as you place the cursor in the omnibox, before you start typing. Chrome is in the process of transitioning to a new service to provide these on-focus suggestions. For most users on desktop versions of Chrome, the request and complete set of suggestions are retained on Google servers in order to further improve and personalize the feature. When the URL that triggered the set of suggestions is deleted from your history, the set of suggestions will stop influencing suggestions personalized to you, and will be deleted; otherwise they are retained in your Google account for a year. For a small portion of users on desktop versions of Chrome, and users on mobile versions of Chrome, the logging described in the previous paragraphs apply except that URLs are never included in the 2% sampling of log data.

On Android, your location will also be sent to Google via an X-Geo HTTP request header if Google is your default search engine, the Chrome app has the permission to use your geolocation, and you haven't blocked geolocation for www.google.com (or country-specific origins such as www.google.de). Additionally, if your device has network location enabled (High Accuracy or Battery Saving Device Location mode in Android settings), the X-Geo header may also include visible network IDs (WiFi and Cell), used to geocode the request server-side. The X-Geo header will never be sent in Incognito mode. HTTPS will be required to include this header in the request. You can learn more about how to control the Android OS location sharing with apps on [this article](#) for Nexus, or find your device [here](#) if you do not use a Nexus. How to control location sharing with a site within Chrome is written in [this article](#). See the [Geolocation](#) section of this whitepaper for more information on default geolocation permissions.

Additionally, if Google is your default search engine and you have enabled sync, omnibox may also show suggestions for your Google Drive files. You can turn this functionality off by disabling the "Drive suggestions" option in the "Sync and Google services" section of Chrome's settings.

If you use a non-Google search provider as your default search engine, queries are sent and logged under that provider's privacy policy.

Additionally, when you use the omnibox to search for a single word, Chrome may send this word to your DNS server to see whether it corresponds to a host on your network, and may try to connect to the corresponding host. This gives you the option to navigate to that host instead of searching. For example, if your router goes by the hostname "router", and you type "router" in the omnibox, you're given the option to navigate to <https://router/>, as well as to search for the word "router" with your default search provider. This feature is not controlled by the "Use a prediction service to help complete searches and URLs..." option because it does not involve sending data to your default search engine.

Network predictions

Chrome uses a prediction service to load pages more quickly. The prediction service uses navigation history and local heuristics to predict which resources and pages are likely to be needed next, and it initiates actions such as DNS prefetching, TCP and TLS preconnection, and prefetching of web pages. To [turn off](#) network predictions, uncheck "Preload pages for faster browsing and searching" in the "Privacy and security > More" section of Chrome's settings on desktop, in the "Privacy" section of Chrome's settings on Android, and in the "Bandwidth" section of Chrome's settings on iOS.

To improve load times, the browser can be asked to prefetch links that you might click next. Chrome supports five types of prefetching:

- Chrome prefetching - can be initiated by Chrome itself whenever it detects a search query typed in the omnibox, a likely beginning of a URL you type often in the omnibox, or when you have Lite mode enabled and are visiting Google Search.
- Webpage prefetching - requested by one web page to prefetch another
- AMP prefetching - can be requested only by the Google Search App on Android to prefetch several accelerated mobile pages (AMP) articles and display them later in a Chrome Custom Tab
- CustomTabs prefetching - any Android app can request to prefetch several URLs to speed up displaying them later in a Chrome Custom Tab
- Privacy-preserving search result link prefetching - for Lite mode users

Controlling the feature. All prefetching types except webpage prefetching are controlled by Chrome's prediction service setting. Webpage prefetching is allowed regardless of whether Chrome's network prediction service feature is enabled.

Handling of cookies. Except for the Lite mode-only prefetching case, the prefetched site is allowed to set and read its own cookies even if you don't end up visiting the prefetched page, and prefetching is disabled if you have chosen to block third-party cookies. In the Lite mode-only case, prefetching is disabled if you have a cookie for the site, and the site can only set a cookie once you click on the link that was prefetched (see the [Lite mode](#) section for more details).

Javascript execution. For AMP prefetching the page is fully rendered and Javascript is also executed. For the remaining types of prefetching Javascript is not executed.

If Google is set as your default search engine, Chrome will try to determine the most appropriate locale for Google search queries conducted from the [omnibox](#) in order to give you relevant search results based on your location. For example, if you were in Germany, your omnibox searches may go through google.de instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTPS request to google.com would be (see the [description of “server logs” in the privacy key terms](#) for details). If you do not have any cookies from google.com, this request will not create any.

New Tab page

The Chrome New Tab page may display suggestions for websites that you might want to visit.

In order to help you get started, Chrome may suggest content that is popular in your country or region. Chrome uses your IP address to identify your country or region.

Chrome tries to make personalized suggestions that are useful to you. For this, Chrome uses the sites you have visited from your local browsing history. On Android, the most popular languages of the sites you visited may also be sent to Google to provide suggestions in languages you prefer to read, and the device display DPI may be sent to format content for your device. To save data, Chrome may additionally send a hash of the content that Google provided to you the last time, so that you only download content when there is something new.

If you are signed into Chrome, suggestions are *also* based on data stored in your Google account activity. You can control the collection of data in your Google account at [Activity controls](#) and manage your account activity at [My Activity](#). For example, if you sync your browsing history and have enabled its use in your Web & App activity, Google may suggest sites that relate to sites you have visited in the past. Chrome measures the quality of suggestions by sending Google information about the sets of suggestions that were displayed, and those that were selected.

On the desktop version of Chrome, you may also manually add shortcuts to websites that you regularly visit, or edit Chrome’s existing website suggestions. After you add, edit, or delete a shortcut to a website, the Chrome New Tab page will not suggest any new websites to you.

Suggestions generated from your browsing history will be removed once you clear your browsing history. However, if you customized your suggestions, they will not be removed.

For Chrome on Android, in certain countries, Chrome may download the content of the New Tab page suggestions from Google, for use while offline. Chrome sends to Google a cookieless request with the URL for each suggestion, along with Chrome’s user agent string, in order to render the content. You can remove downloaded content by clearing Chrome’s cache data, or by opening the Downloads menu and [selecting individual pages to delete](#). You can disable this feature by disabling “Download articles for you on Wi-Fi” in Chrome’s Downloads settings.

For Chrome on Android, if you’re signed in to Chrome, your preferences for the suggested articles can be modified or removed using the “Manage Interests” option from any suggested article menu. Your preferences will be sent to Google so that better suggestions are provided to you in the future. For example, if you indicate that you’re not interested in a particular topic or publisher, suggestions about that topic or publisher will not be shown in the future.

For desktop and Android versions of Chrome, when you open a new tab, Chrome loads a New Tab page customized by your default search engine (e.g., google.com) if it’s available. This page is preloaded in the background and refreshed periodically so that it opens quickly. Your IP address and cookies, as well as your current browser theme, are sent to your search engine with each refresh request so that the New Tab page can be correctly displayed. See the [Embedded Search API](#) for more details. Your search engine may also record your interactions with the New Tab page.

The New Tab page content may be designed by your default search provider. Suggested websites are embedded by Chrome into the New Tab page in a way that does not expose them to your default search provider.

If your default search provider is Google, the New Tab page also contains a web address and search bar that behaves like the [omnibox](#).

This information about the New Tab page may not apply if you've installed an extension that [overrides the New Tab page](#).

Touch to Search

If you've enabled "Touch to Search" on Chrome Mobile you can search for terms by tapping them.

When you tap a word, the word, the surrounding text, and the home country of your device's SIM card are sent to Google to identify recommended search terms (for example, tapping on "whale" on a site about the blue whale would lead to showing "blue whale"). The tapped word is logged in accordance with standard Google logging policies, and the surrounding text and home country are logged only when the page is already in Google's search index. If you have turned on “Make searches and browsing better”, the URL of the page is also sent and logged, and is used to improve your query suggestions.

When Google returns a search suggestion, a card "peeks through" at the bottom of the screen, showing the suggested search term. Opening this card is considered a regular search and navigation on Google, so standard logging policies apply.

Long-pressing on a word opens a peeking card for the selected word. No communication with Google occurs until the card is opened, and no surrounding text is sent. Saying “Ok Google” after long-pressing on a word provides the word and its surrounding text as context for the Google Assistant.

Touch to Search is enabled in a limited mode by default: potentially privacy-sensitive data, such as the URL and surrounding text, is not sent for HTTPS pages. Touch to Search can be fully enabled and disabled in the card or in the Chrome privacy settings.

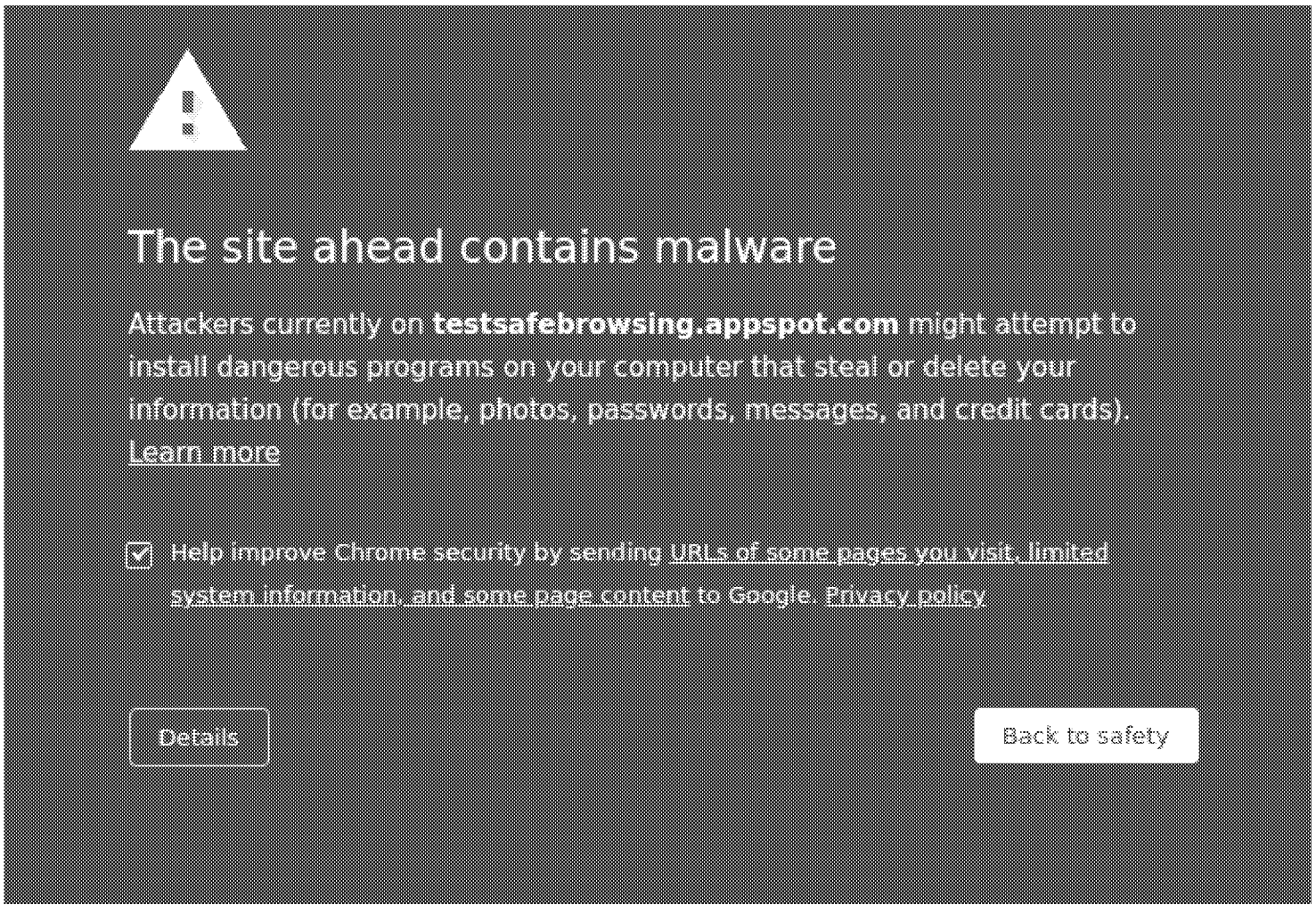
Safe Browsing protection

Google Chrome includes an optional feature called "Safe Browsing" to help protect you against [phishing](#), [social engineering](#), [malware](#), [unwanted software](#), malicious ads, intrusive ads, and abusive websites or extensions. You can find more information at [safebrowsing.google.com](#) about how Safe Browsing protects you in Chrome and other Google products. Safe Browsing is designed specifically to protect your privacy and is also used by other popular browsers. This feature is not available on the iOS version of Chrome.

You can find settings for Safe Browsing in the “Privacy and security > More” section of Chrome’s settings. When Safe Browsing is enabled in Chrome, Chrome contacts Google’s servers periodically to download the most recent Safe Browsing list of unsafe sites including sites associated with phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or Chrome extensions. The most recent copy of this list is stored locally on your system. Chrome checks the URL of each site you visit or file you download against this local list. If you navigate to a URL that appears on the list, Chrome sends a partial URL fingerprint (the first 32 bits of a SHA-256 hash of the URL) to Google for verification that the URL is indeed dangerous. Chrome also sends a partial URL fingerprint when a site requests a potentially dangerous permission, so that Google can protect you if the site is malicious. Google cannot determine the actual URL from this information.

In addition to the URL check described above, Chrome also conducts client-side checks. If a website looks suspicious, Chrome sends a subset of likely phishing and social engineering terms found on the page to Google, in order to determine whether the website should be considered malicious. Chrome can also help protect you from phishing if you type one of your previously saved passwords into an uncommon site. In this case Chrome sends the URL and referrers of the page to Google to see if the page might be trying to steal your password.

If you encounter a website that is on Chrome’s Safe Browsing list, you may see a warning like the one shown below.



You can [visit our malware warning test page](#) or [social engineering warning test page](#) to see the above example in action. For more information about the warning pages, see [Manage warnings about unsafe sites](#).

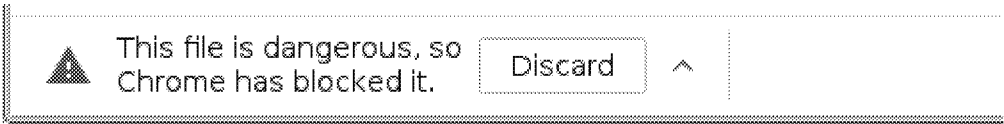
Additionally, if you've opted into “Make Searches and Browsing Better (sends URLs of the pages you visit to Google)”, Chrome sends a request to Safe Browsing each time you visit a page that isn't in Chrome’s local list of safe sites in order to gather the latest reputation of that website. If the website is deemed unsafe by

You can also opt in to reporting additional [data relevant to security](#) to help improve Safe Browsing and security on the Internet. You can opt in by turning on the “Help improve Chrome security” setting in the “Privacy and security > More” section of Chrome's settings. You can also opt in from the warning page shown above. If you opt in, Chrome will send an incident report to Google every time you receive a warning, visit a suspicious page, and on a very small fraction of sites where Chrome thinks there could be threats, to help Safe Browsing learn about the new threats you may be encountering. The reports are sent to Google over an encrypted channel and can include URLs, headers, and snippets of content from the page and they never include data from browsing you do in Incognito mode. If Chrome discovers unwanted or malicious software on your machine, the reports may also include details about malicious files and registry entries. This data is used only to improve Safe Browsing and to improve security on the Internet. For example, Chrome reports some [SSL certificate](#) chains to Google to help improve the accuracy of Chrome’s SSL warnings.

Please be aware that if you disable the Safe Browsing feature, Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software. We don't recommend turning it off.

If you are a webmaster, developer, or network admin, you can find more relevant information about Safe Browsing on [this page](#).

Safe Browsing also protects you from abusive extensions and malicious software. When Chrome starts, and on each update of the Safe Browsing list, Chrome scans extensions installed in your browser against the Safe Browsing list. If an extension on the list is found, Chrome will disable the extension, offer you relevant information and may provide an option for you to remove the extension or re-enable it. Chrome also sends the particular extension ID to Safe Browsing. If you attempt to download a file on Chrome’s Safe Browsing list, you’ll see a warning like this one:



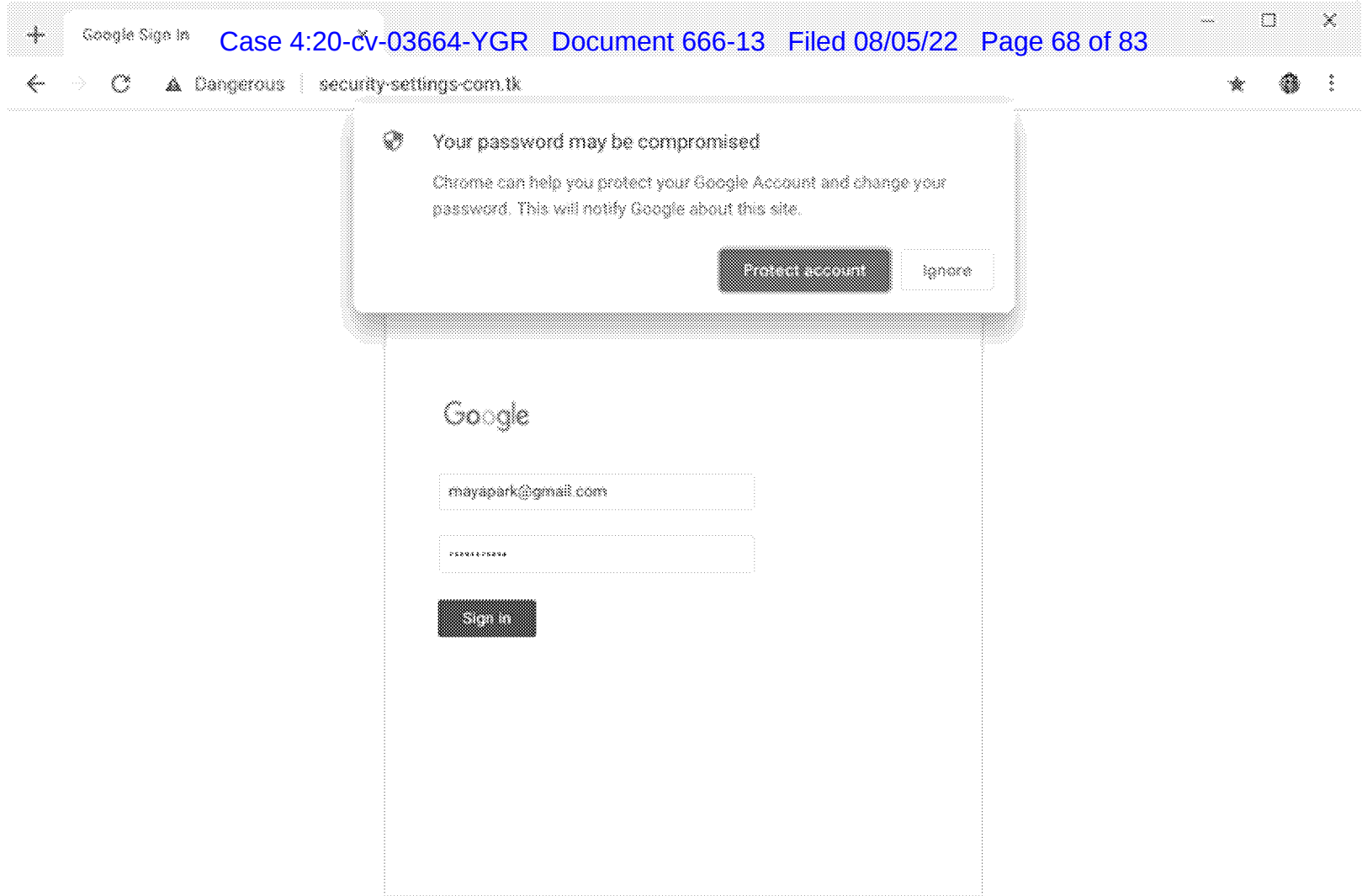
To warn you about potentially dangerous files, like the picture shown above, Chrome checks the URL of potentially dangerous file types you download against a list of URLs that have been verified. Potentially dangerous file types include both executables and commonly-abused document types. This list is stored locally on your computer and updated regularly. Chrome does not send information to Google for files you download from URLs in this list, or if the file is signed by a verified publisher. For all other unverified potentially dangerous file downloads, Chrome sends Google the information needed to help determine whether the download is harmful, including some or all of the following: information about the full URL of the site or file download, all related referrers and redirects, code signing certificates, file hashes, and file header information. Chrome may then show a warning like the one pictured above.

If you are enrolled in [Google's Advanced Protection Program](#), Chrome will show you additional warnings when you download files but where Safe Browsing is unable to ascertain they are safe.

Chrome helps protect you against password phishing by checking with Google when you enter your password on an uncommon page. Chrome keeps a local list of popular websites that Safe Browsing found to be safe. If Chrome detects that you have entered your Google account password or one of your passwords stored in Chrome’s password manager on a website that’s not on the list, it sends a request to Safe Browsing to gather the reputation of that website. The verdict received from Safe Browsing is usually cached on your device for 1 week. For users who have enabled the "Help improve Chrome security" setting, Chrome will ignore the list of popular websites for a small fraction of visits, to test the accuracy of that list.

If the reused password is your Google account password and the verdict for the website is that it is phishing, Chrome will suggest that you change your Google account password to avoid losing access to your account.

If you sync your browsing history without a sync passphrase, or if you accept the “Protect account” option from the dialog shown below, Chrome sends a request to Google to protect your account. This request contains the URL where the phishing attempt happened, and the verdict received from Safe Browsing.



If you've opted into "Help improve Chrome security", Chrome also sends a request to Safe Browsing each time you start to enter a password on a page that isn't in Chrome's local list. In addition, the request Chrome sends to Safe Browsing to determine the reputation of the website on which you reuse your password includes the list of websites for which you saved this password in Chrome's password manager (but not the password itself).

If Chrome detects that your settings have been tampered with, Chrome reports the URL of the last downloaded potentially dangerous file, and information about the nature of the possible tampering, to the Safe Browsing service.

For some downloads, Chrome may ask you to opt in to reporting to Google Safe Browsing some data relevant to security, in order to improve the quality of download protection. Once you've opted in, some downloaded files that are suspicious will be sent to Google for investigation each time they are encountered. You can change this opt-in setting at any time in the Chrome settings.

Chrome asks your permission before using certain web features (APIs) that might have associated risks. Some sites trigger these permission requests in ways users find undesirable or annoying. On these sites Chrome may send the partial URL fingerprint to Google to verify if a less intrusive UI should be used to surface the request.

Furthermore, to improve the safety and utility of Chrome permissions, Chrome may anonymously report the domains on which you grant, reject and revoke permissions or ignore or dismiss permission prompts. This happens only if you are a Safe Browsing user and have activated syncing your browsing history and settings with Google without a custom passphrase.

For all Safe Browsing requests and reports, Google logs the transferred data in its raw form and retains this data for up to 30 days. Google collects standard log information for Safe Browsing requests, including an IP address and one or more cookies. After at most 30 days, Safe Browsing deletes the raw logs, storing only calculated data in an anonymized form that does not include your IP addresses or cookies. Additionally, Safe Browsing requests won't be associated with your Google Account. They are, however, tied to the other Safe Browsing requests made from the same device.

For Chrome on iOS 13 and later, Apple allows for connecting to multiple Safe Browsing services. This means that Chrome may connect to a third-party Safe Browsing service instead of the Google one. Apple determines which Safe Browsing service to connect to based on factors like your device locale.

Unwanted software protection

The Windows version of Chrome is able to detect and remove certain types of software that violate [Google's Unwanted Software Policy](#). If left in your system, this software may perform unwanted actions, such as changing your Chrome settings without your approval. Chrome periodically scans your device to detect potentially unwanted software. In addition, [if you have opted in to automatically report details of possible security incidents to Google](#), Chrome will report information about unwanted software, including relevant file metadata and system settings linked to the unwanted software found on your computer.

If you perform an unwanted software check on your computer from the Settings page, Chrome reports information about unwanted software and your system. System information includes metadata about programs installed or running on your system that could be associated with harmful software, such as: services and processes, scheduled tasks, system registry values commonly used by malicious software, command-line arguments of Chrome shortcuts, Windows proxy settings, and software modules loaded into Chrome or the network stack. You can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the scan.

If unwanted software is detected, Chrome will offer you an option to clean it up by using the Chrome Cleanup Tool. This will quarantine detected malicious files, delete harmful extensions and registry keys, and reset your settings. The Chrome Cleanup Tool also reports information about unwanted software and your system to Google, and again you can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the cleanup.

This data is used for the purpose of improving Google’s ability to detect unwanted software and offer better protection to Chrome users. It is used in accordance with Google’s Privacy Policy and is stored for up to 14 days, after which only aggregated statistics are retained.

Navigation error tips

Google Chrome can show tips to help guide you to the page you were trying to reach in cases where the web address cannot be found, a connection cannot be made, the server returns a very short (under 512 byte) error message, or you've navigated to a parked domain.

Google Chrome will first check the address against a locally-stored list of suspected parked domains. If there is a match, Chrome sends a partial fingerprint (a hash prefix) of the URL to Google for verification that the domain is indeed parked. This uses the same methodology as the Safe Browsing service (see the “Safe Browsing protection” section, above).

In the case of other navigation errors, the URL of the web page you’re trying to reach is stripped of all GET parameters, and then sent to Google in order to retrieve navigation tips. This information is logged and anonymized in the same manner as Google web searches. The logs are used to ensure and improve the quality of the feature.

Additionally, to provide you with more informative error messages when a domain name cannot be found, Chrome will investigate the underlying cause by attempting to resolve “google.com” using both Google Public DNS and the default DNS service configured for your system.

In the event that Chrome detects SSL connection timeouts, certificate errors, or other network issues that might be caused by a captive portal (a hotel's WiFi network, for instance), Chrome will make a cookieless request to https://www.gstatic.com/generate_204 and check the response code. If that request is redirected, Chrome will open the redirect target in a new tab on the assumption that it's a login page. Requests to the captive portal detection page are not logged.

You can disable navigation error tips by unchecking "Show suggestions for similar pages when a page can't be found" in the "Sync and Google services" section of Chrome's settings.

Offline Indicator

On Android versions Lollipop and older, when Chrome detects a network change, it sends a cookieless request to http://connectivitycheck.gstatic.com/generate_204 or http://clients4.google.com/generate_204 to determine whether you’re offline and display an offline indicator.

Software updates

Desktop versions of Chrome and the Google Chrome Apps Launcher use Google Update to keep you up to date with the latest and most secure versions of software. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is open source.

Google Update requests include information necessary for the update process, such as the version of Chrome, its release channel, basic hardware information, and update errors that have been encountered. The update requests also send Google information that helps us understand how many people are using Google Chrome and the Chrome Apps Launcher – specifically, whether the software was used in the last day, the number of days since the last time it was used, the total number of days it has been installed, and the number of active profiles. Google Update also periodically sends a non-unique four-letter tag that contains information about how you obtained Google Chrome. This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is the same as everyone who obtained Google Chrome the same way.

Because Chrome OS updates the entire OS stack, Google Update on Chrome OS also sends the current Chrome OS version and hardware model information to Google in order to ensure that the correct software updates and hardware manufacturer customizations such as apps, wallpaper, and help articles are delivered. This information is not personally identifiable, and is common to all users of Chrome OS on the same revision of device.

Unlike the desktop versions of Chrome, the delivery and management of updates for mobile versions of Chrome are managed through the app stores for Android and iOS. Mobile versions of Chrome utilize the servers described above for counting active installations.

Chrome extensions and applications that you’ve installed are kept up to date with a similar system used for updating desktop versions of Chrome. These update requests include similar information (such as the application ID, when the application was last used, and how long it’s been installed). We use these requests to determine the aggregate popularity and usage of applications and extensions. If you are using an extension or application restricted to a certain audience,

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which can be updated independently. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (e.g., "fmeadaodfnidclnjhlkdgjkolmhmfofk"). An update request for a component contains this ID, the hash of the previous download (called a "fingerprint"), and the component's version. Because every installation has the same ID, and downloads of the same component have the same fingerprint, none of this information is personally identifiable.

If you install web apps on an Android device, a Google server is responsible for creating a native Android package that can be verified for authenticity by Chrome. When Chrome is updated or notices that the web app's manifest has changed, Chrome asks the server for a new version of the Android package in a cookieless request. If the information needed to create the native Android package cannot be acquired by the server (e.g., because the information is behind a corporate firewall), Chrome sends it to Google and an Android package is created that is unique to you. It contains a unique and random identifier that is not tied to your identity.

Chrome may also download and run a binary executable (e.g., as part of the software update or to improve Safe Browsing protection). These executables are cryptographically signed and verified before execution. Chrome may download further static resources like dictionaries on demand to reduce the size of the installer.

On Windows and OS X versions of Chrome, the recovery component tries to repair Google Update when it's broken. After the relevant binary is executed, Google Update uploads statistics on the actions that were performed. These statistics contain no personally identifiable information.

Network time

On desktop platforms, Chrome uses network time to verify SSL certificates, which are valid only for a specified time. At random intervals or when Chrome encounters an expired SSL certificate, Chrome may send requests to Google to obtain the time from a trusted source. These requests are more frequent if Chrome believes the system clock is inaccurate. These requests contain no cookies and are not logged on the server.

Counting installations

In order to measure the success rate of Google Chrome downloads and installations of the Windows version of Google Chrome, a randomly-generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. A new token is generated for every install. It is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

For Chrome to know how many active installations it has, the mobile version of Chrome sends a ping to Google with a salted hash of a device identifier on an ongoing basis. The desktop version of Chrome does not send any stable identifier to count active installations. Instead an anonymous message to Google with a timestamp of the last ping is used to infer number of active installations.

Measuring effectiveness of a promotion

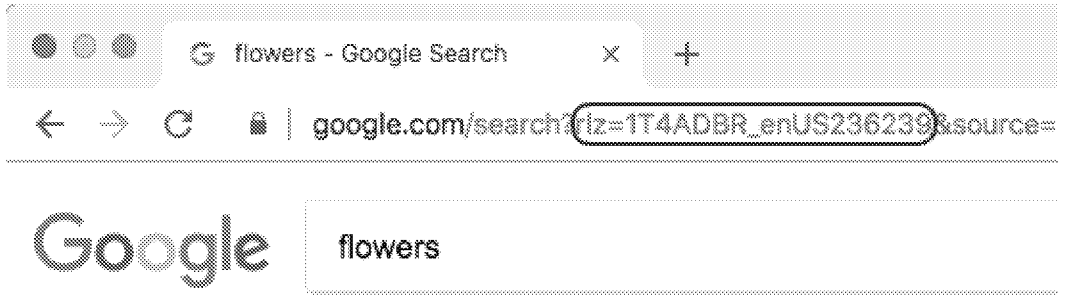
Chrome utilizes two measurements to understand how effective a promotional campaign has been: how many Chrome installations are acquired through a promotional campaign, and how much Chrome usage and traffic to Google is driven by a campaign.

To measure installations or reactivations of Chrome through a campaign, Chrome will send a token or an identifier unique to your device to Google at the first launch of Chrome, as well as the first search using Google. On desktop versions of Chrome, a token unique to your device is generated. The same token will be sent if Chrome is later reinstalled at first launch and at first use of the Omnibox after reinstallation or reactivation. Rather than storing the token on the computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner. On iOS, Chrome uses the IDFA for counting installations acquired by a campaign, and it can be reset in iOS settings.

To measure searches and Chrome usage driven by a particular campaign, Chrome inserts a promotional tag, not unique to you or your device, in the searches you perform on Google. This non-unique tag contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. For desktop versions of Chrome, Chrome generates a promotional tag, if the promotional installation token described in the previous paragraph indicates that Chrome has been installed or reactivated by a campaign on a device which has not been associated with any campaign yet. For Chrome on Mobile, a promotional tag is always sent regardless of the source of installations.

The promotional tag is generated using a software library called "RLZ" and looks similar to "1T4ADBR_enUS236US239". The RLZ library was fully open-sourced in June 2010. For more information, please see the In the Open, for RLZ post on the Chromium blog and the article "How To Read An RLZ String". On Android, this promotional tag can also be a readable string like "android-hms-tmobile-us" instead of an RLZ string, and is not unique to either you or your device.

This non-unique promotional tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to measure the searches and Chrome usage driven by a particular promotion.

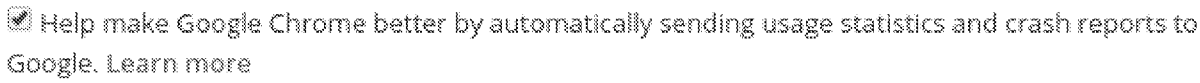


If usage statistics and crash reports are enabled, the RLZ string is sent along with the report. This allows us to improve Chrome based on [variations](#) that are limited to specific geographic regions.

For the desktop version of Chrome, you can opt-out of sending this data to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome. To opt-out of sending the RLZ string in Chrome OS, press Ctrl + Alt + T to open the [crosh shell](#), type rlz disable followed by the enter key, and then reboot your device.

Usage statistics and crash reports

Chrome has a feature to automatically send [usage statistics and crash reports](#) to Google in order to help improve Chrome’s feature set and stability.



Usage statistics contain information such as system information, preferences, user interface feature usage, responsiveness, performance, and memory usage. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs or personal information depending on what was happening at the time of the crash. This feature is enabled by default for Chrome installations of version 54 or later. You can control the feature in the "Sync and Google services" section of Chrome's settings.

When this feature is enabled, Google Chrome stores a randomly generated unique token on your device, which is sent to Google along with your usage statistics and crash reports. The token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics. This token is deleted when the feature is disabled and a new token is regenerated when the feature is enabled again.

By default, the usage statistics do not include any personal information. However, if you're signed in to Chrome and have enabled Chrome sync, Chrome may combine your declared [age and gender](#) from your Google account with our statistics to help us build products better suited for your demographics. This demographic data is not included in crash reports.

Along with usage statistics and crash reports, Chrome also reports anonymous, randomized data that is constructed in a manner which is not linked to the unique token, and which ensures that [no information can be inferred about any particular user's activity](#). This data collection mechanism is summarized on the [Google research blog](#), and full technical details have been published in a [technical report](#) and presented at the 2014 ACM Computer and Communications Security conference.

Chrome will also anonymously report to Google if requests to websites operated by Google fail or succeed in order to detect and fix problems quickly.

If you have also turned on “Make searches and browsing better (Sends URLs of pages you visit to Google)” in the “Sync and Google services” section of Chrome’s settings, Chrome usage statistics include information about the web pages you visit and your usage of them. The information will also include the URLs and statistics related to downloaded files. If you sync [extensions](#), these statistics will also include information about the extensions that have been installed from Chrome Web Store. The URLs and statistics are sent along with a unique device identifier that can be reset by turning off “Make searches and browsing better” in the “Sync and Google services” section of Chrome’s settings or by turning off usage statistics and crash reports. The usage statistics are not tied to your Google account. Google only stores usage statistics associated with published extensions, and URLs that are known by Google's web crawlers. We use this information to improve our products and services, for example, by identifying web pages which load slowly; this gives us insight into how to best improve overall Chrome performance. We also make some statistics available externally, through efforts like the [Chrome User Experience Report](#). Externally published reports are conducted in highly aggregated manner to not reveal individual user's identity.

On iOS, if you are syncing your browsing history without a sync passphrase, Chrome reports usage for certain URLs that other Google apps could open. For example, when you tap on an email address, Chrome presents a dialog that allows you to choose between opening with Google Gmail or other mail apps installed on your device. The usage information also includes which apps were presented to you, which one was selected, and if a Google app was installed. Chrome does not log the actual URL tapped. If you are signed in, this usage is tied to your Google account. If you are signed out, the information is sent to Google with a unique device identifier that can be regenerated by resetting the Google Usage ID found in Chrome settings. The raw reports are deleted within 60 days, after which only the aggregated statistics remain.

In Chrome on Android and Desktop, when you have "send usage statistics" enabled, you may be randomly selected to participate in surveys to evaluate consumer satisfaction with Chrome features. If you are selected, Chrome requests a survey from Google for you. If a survey is available, Chrome then asks you to answer the survey and submit responses to Google.

The survey also records basic metrics about your actions, such as time spent looking at the survey and elements that the user clicked. These metrics are sent to Google even if you do not fully complete the survey.

Google uses strategies to ensure that surveys are spread evenly across users and not repeatedly served to a single user. On Android, Chrome stores a randomly generated unique token on the device. On Desktop, Chrome uses a cookie to connect with the server. This token or cookie is used solely for the survey requests and does not contain any personal information. If you disable sending usage statistics, the token or cookie will be cleared.

Suggestions for spelling errors

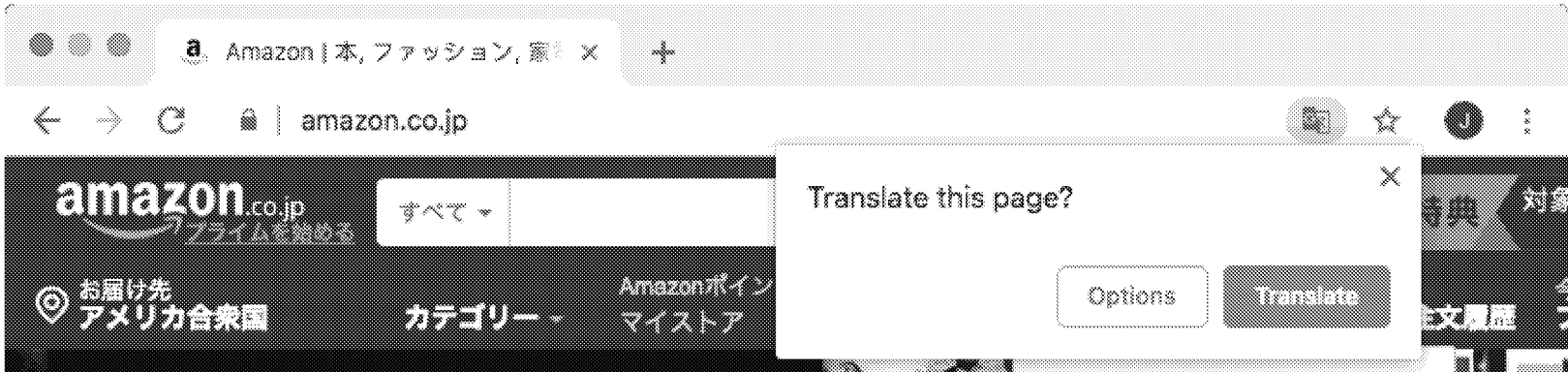
Desktop versions of Chrome can provide smarter spell-checking by sending text you type into the browser to Google's servers, allowing you to apply the same spell-checking technology that’s used by Google products like Docs. If this feature is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser’s default language. Google returns a list of suggested spellings that are displayed in the context menu. Cookies are not sent along with these requests. Requests are logged temporarily and anonymously for debugging and quality improvement purposes.

This feature is disabled by default; to turn it on, click “Ask Google for suggestions” in the context menu that appears when you right-click on a misspelled word. You can also turn this feature on or off with the “Enhanced spell check” checkbox in the “Sync and Google services” section of Chrome settings. When the feature is turned off, spelling suggestions are generated locally without sending data to Google's servers.

Mobile versions of Chrome rely on the operating system to provide spell-checking.

Translate

Google Chrome’s built-in translation feature helps you read more of the Web, regardless of the language of the web page. The feature is enabled by default.



Translation can be disabled at any time in Chrome’s settings.

Language *detection* is done entirely using a client-side library, and does not involve any Google servers. For *translation*, the contents of a web page are only sent to Google if you decide to have it translated. You can do that on an individual basis on each page that shows a translation option or for all pages in a specific language by choosing “Always translate” in the Translate UI. Additionally, you can do so by clicking on a translated search result on the Google Search Results Page.

If you do choose to translate a web page, the text of that page is sent to [Google Translate](#) for translation. Your cookies are not sent along with that request and the request is sent over SSL. This communication with Google's translation service is covered by the [Google privacy policy](#).

If you’ve chosen to sync your Chrome history, statistics about the languages of pages you visit and about your interactions with the translation feature will be sent to Google to improve Chrome’s understanding of the languages you speak and when Chrome should offer to translate text for you.

Image Descriptions for screen reader users

Chrome can provide automatic descriptions for users who are visually impaired by sending the contents of images on pages you visit to Google's servers. This feature is only enabled when Chrome detects that the user has a screen reader running and if the user explicitly enables it in the page context menu. Cookies are not sent along with these requests. Requests are not logged.

Sign In to Chrome and sync

You have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.

On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. If you are signed in to Chrome, Chrome may offer to save your payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can turn off Chrome sign-in.

When you're signed-in and have enabled sync with your Google Account, your personal browsing data information is saved in your Google Account so you may access it when you sign in and sync to Chrome on other computers and devices. Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions, addresses, phone numbers, payment methods, and more. In advanced sync settings, you can choose which types of data to synchronize with this device. By default, all syncable data types are enabled. You can turn sync on or off in the "You and Google" section of Chrome settings.

If you have turned on sync and signed out of the account you are syncing to, sync will pause sending all syncable data to Google until you sign back in with the same account. Some sync data types (such as bookmarks and passwords) that are saved locally while sync is paused will automatically be synced to your account after you sign back in with the same account.

On mobile versions of Chrome, you can sign into or sign out of Chrome from Chrome settings. Signing into Chrome will also turn on sync. This can be done for any account that has already been added to the mobile device without authenticating again.

On both desktop and mobile, signing into Chrome keeps you signed into Google web services until you sign out of Chrome. On mobile, signing into Chrome will keep you signed in with all Google Accounts that have been added to the device. On desktop, it will keep you signed in with all Google Accounts that you added from a Google web service, unless you have set "Keep local data only until you quit your browser" in your cookie settings.

On Android and desktop, Chrome signals to Google web services that you are signed into Chrome by attaching an X-Chrome-Connected and/or C-Chrome-ID-Consistency-Request header to any HTTPS requests to Google-owned domains. On iOS, the CHROME_CONNECTED cookie is used instead. This allows those Google web services to update their UI accordingly. If you are using a managed device, your system admin may disable the sign in feature or require that data be deleted when you disconnect your account.

Users can share phone numbers and text between their devices (mobile or desktop) when they are signed-in to Chrome. The transferred data is encrypted during transit and Google cannot read or store the content. To let users select the device to share with, Chrome collects the following information about devices on which a user is signed-in and stores that in the user's Google account: device manufacturer, model number, Chrome version, OS, and device type.

Google uses your personal synchronized data to provide you a consistent browsing experience across your devices, and to customize features in Chrome. You can manage your synchronized history by going to chrome://history in your Chrome browser. If "Include history from Chrome and other apps in your Web & App Activity" is checked on the Web & App Activity controls page, Google also uses your synchronized browsing data to provide personalized Google products and services to you. You can change your preference any time, and manage individual activities associated with your Google account.

The paragraph above describes the use of your personal browsing history. Google also uses aggregated and anonymized synchronized browsing data to improve other Google products and services. For example, we use this information to improve Google Search by helping to detect mobile friendly pages, pages which have stopped serving content, and downloads of malware.

If you would like to use Google's cloud to store and sync your Chrome data without allowing any personalized and aggregated use by Google as described in the previous paragraphs, you can choose to encrypt all of your synced data with a sync passphrase. If you choose this option, it's important to note that Google won't have access to the sync passphrase you set; we won't be able to help you recover data if you forget the passphrase. Regardless of how you choose to encrypt your data, all data is always sent over secure SSL connections to Google's servers.

Google will store the metadata about the days on which sync was running to improve other Google products and services.

If you're signed into Chrome and are syncing passwords and/or other types of login credentials without a sync passphrase, these credentials are stored in your Google Account. Chrome may help you sign in with credentials you've saved in Android apps on websites that are associated with the respective apps. Likewise, credentials you've saved for websites can be used to help you sign into related Android apps. You can view the credentials you've saved in Chrome and Android by visiting passwords.google.com in any browser. If you've saved credentials for Android applications, Chrome periodically sends a cookieless request to Google to get an updated list of websites that are associated with those applications. To stop websites and Android apps from automatically signing in using credentials you previously saved, you can turn off Auto Sign-In on passwords.google.com or in Chrome settings under "Manage passwords". For more details see this article.

To make the history page easier to use, Chrome displays favicons of visited URLs. For Chrome browsing history from your other devices, these favicons are fetched from Google servers via cookieless requests that only contain the given URL and device display DPI. Favicons are not fetched for users with sync passphrase.

On the iOS version of Chrome, if you sync your browsing history without a sync passphrase and your browser's usage statistics and crash reports setting is also enabled, your usage statistics and crash reports will include statistics about the pages you visit. You can read more in the Usage statistics and crash reports

All data synchronized through Google’s servers is subject to [Google’s Privacy Policy](#). To get an overview of the Chrome data stored for your Google Account, go to the [Chrome section of Google Dashboard](#). That page also allows you to stop synchronization completely and delete all sync data from Google’s servers.

Autofill and Password Management

Google Chrome has a [form autofill feature](#) that helps you fill out forms on the web more quickly. Autofill is enabled by default, but it can be turned off at any time in Chrome’s settings.

If Autofill is enabled and you encounter a web page containing a form, Chrome sends some information about that form to Google. This information includes a hash of the web page’s hostname, as well as form identifiers (such as field names), and the basic structure of the form. In response, Chrome receives a prediction of each field’s data type (for example, “field X is a phone number, and field Y is a country”). This information helps Chrome match up your locally stored Autofill data with the fields of the form.

If Autofill is enabled when you *submit* a form, Chrome sends Google some information about the form along with the types of data you submitted. This information includes a hash of the web page’s hostname, as well as form identifiers (such as field names), the basic structure of the form, and the observed data types for the fields (i.e., field X was a phone number, field Y was a country). The values you entered into the form are not sent to Google. This information helps Chrome improve the quality of its form-filling over time.

You can manage your Autofill entries via [Chrome’s settings](#), and you can edit or delete saved information at any time. Chrome will never store full credit card information (card number, cardholder name, and expiration date) without explicit confirmation. In order to prevent offering to save cards you have shown disinterest in saving, Chrome stores the last four digits of detected credit cards locally on the device. If you scan your credit card using a phone camera, the recognition is performed locally.

Chrome may help you sign in to websites with credentials you’ve saved to Chrome’s password manager or Google Smart Lock by autofilling sign-in forms, by offering you an account picker, or by automatically signing you in. You can manage and delete your saved credentials in the “Forms and passwords” section of Chrome’s settings. If you enable [password management](#), the same kind of data about forms as described above is sent to Google to interpret password forms correctly. To enable Chrome to offer password generation that meets site-specific requirements, Chrome uploads a randomized vote on a specific password characteristic to the server once a user-created password is stored. If stored credentials are used for the first time in a username field which was already filled differently by the website itself, Chrome also transmits a short one-byte hash of the prefilled value. This allows Google to classify if the website uses a static placeholder in the username field which can be safely overwritten without deleting valuable user-specific data. Google cannot reconstruct the value from this hash.

When you sign in to a site, Chrome can give you a [warning](#) if the username/password have been exposed as a result of a data breach on some website or app. The feature is available on all platforms but only to the users signed in with a Google account. On Android the feature is only available if sync is also enabled, due to the way the accounts are managed by the OS. Being signed in to a Google account is a technical requirement that prevents abuse of the API. When you sign in to a website, Chrome will send a hashed copy of your username and password to Google encrypted with a secret key only known to Chrome. [No one, including Google, is able to derive your username or password from this encrypted copy](#). From the response, Chrome can tell if the submitted username and password appear in the database of leaked credentials. The final resolution is done locally; Google doesn’t know whether or not the credential is present in the database. The feature can be disabled in settings under Sync and Google services. On desktop and Android versions of Chrome, this feature is not available if Safe Browsing is turned off.

Also, if you choose, you can bring your Autofill data with you to all your Chrome-enabled devices by [syncing it](#) as part of your browser settings (see the “Sign In to Chrome” section of this document). If you choose to sync Autofill information, field values are sent as described in “Sign In to Chrome”; otherwise, field values are not sent.

Payments

When you’re signed into Chrome with your Google Account, Chrome may offer to save payment cards and related billing addresses into payment data under the same Google Account, and include cards from your account among the autofill suggestions on payment web forms. If you’re not signed in, Chrome offers to save your credit cards locally. If the card is not stored locally, you will be prompted for your CVV code or device authentication, such as Touch ID or Windows Hello, each time you use the card. In some versions of Chrome, it is possible to store a card to Google Payments and locally in Chrome at the same time, in which case Chrome will not ask for a CVV or device authentication confirmation. If you have cards stored in this way, their local copies will persist until you sign out of your Google account, at which point the local copy will be deleted from your device. If you choose not to store the card locally, you will be prompted for your CVV code or device authentication each time you use the card. You can [opt out of using device authentication](#) in the Payment methods section of Chrome settings. If you use a card from Google Payments, Chrome will collect information about your computer and share it with Google Payments to prevent fraudulent use of your card.

To delete credit card information saved in Chrome, follow the “Add and edit credit cards” steps in the Autofill article. When you delete a credit card that's also saved in your Google Payments account, you will be redirected to Google Payments to complete the deletion. After your card has been deleted from your Google Payments account, Chrome will automatically remove that card from your Autofill suggestions.

To save a card locally on the device only, while still being signed in to Chrome with a Google Account, you can add a card from the “Add” button in the “Payment methods” section in Chrome settings. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can turn off Chrome sign-in. If you have sync turned on, you can disable syncing payment methods and addresses to Google Pay under “Sync” in Chrome settings. You can also turn the Payments Autofill feature off altogether in settings.

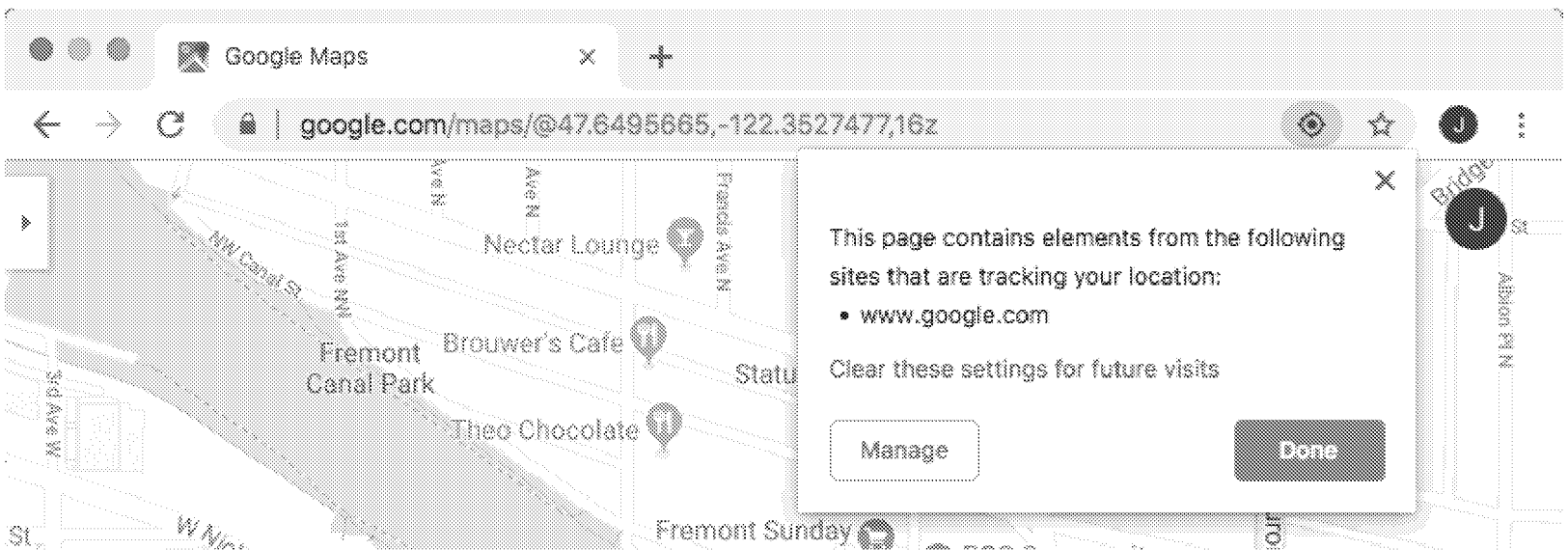
Chrome also supports the PaymentRequest API by allowing you to pay for purchases with credit cards from Autofill, Google Payments, and other payment apps already installed on your device. Google Payments and other payment apps are only available on Android devices. PaymentRequest allows the merchant to request the following information: full name, shipping address, billing address, phone number, email, credit card number, credit card expiration, CVV, and Google Payments credentials. Information is not shared with the merchant until you agree.

Geolocation

Google Chrome supports the Geolocation API, which provides access to fine-grained user location information with your consent.

By default, Chrome will request your permission when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.

Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In Chrome’s settings, by clicking “Site Settings” and scrolling to the “Location” section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

In the Android version of Chrome, your default search engine automatically receives your location when you conduct a search. On the iOS version of Chrome, by default your location is sent to Google if you conduct a search from the omnibox. Read more about how your default search engine handles geolocation and how to manage your settings in the Omnibox section of the whitepaper.

If you do choose to share your location with a web site, Chrome will send local network information to Google (also used by other browsers such as Mozilla Firefox) in order to estimate your location. This local network information can include data about nearby Wi-Fi access points or cellular signal sites/towers (even if you’re not using them), and your computer’s IP address. The requests are logged, and aggregated and anonymized before being used to operate, support, and improve the overall quality of Google Chrome and Google Location Services.

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see “Practical Privacy Concerns in a Real World Browser” written by two Google Chrome team members.

Speech to text

Chrome supports the Web Speech API, a mechanism for converting speech to text on a web page. It uses Google's servers to perform the conversion. Using the feature sends an audio recording to Google (audio data is not sent directly to the page itself), along with the domain of the website using the API, your default browser language and the language settings of the website. Cookies are not sent along with these requests.

Google Assistant on Chrome OS devices

The Google Assistant is integrated into some models of Chrome OS devices. If you opt in to the feature, Chrome OS listens for you to say "Ok Google" and sends the audio of the next thing you say, plus a few seconds before, to Google. Detection of the phrase "Ok Google" is performed locally on your computer, and the

audio is only sent to Google after it detects "Ok Google." You can enable or disable this feature in Google Assistant Settings.

Case 4:20-cv-03664-YGR Document 666-13 Filed 08/05/22 Page 76 of 83

Enabling this feature in Chrome Settings will cause Chrome to listen whenever the screen is unlocked. On Chrome OS devices with a local audio processor, the device also listens when the device is asleep. On these devices, The Google Assistant feature only works if Voice & Audio Activity is enabled for your Google account. Chrome will prompt you to enable Voice & Audio Activity for the associated Google account if it is disabled.

Once the audio has been converted to text, a search with that text is submitted to Google. If you have used the “Ok Google” search before on a device but turned off Voice & Audio Activity later, your device is still capable of processing your voice and sending the audio to Google but the voice is deleted shortly thereafter.

You can determine your Chrome OS device’s behavior by examining the text in the "Search and Assistant" section of settings.

Google Assistant on Android devices

You can quickly complete tasks on the web using the Google Assistant in Chrome on certain Android devices . If you opt-in to this feature, you can speak to the Google Assistant and ask it to search websites. It also can fill out forms on your behalf, or speed up the checkout experience.

For example, if you issue a command to the Google Assistant e.g. “search Wikipedia for Henry VIII”, the Google Assistant in Chrome will respond by opening Chrome to Wikipedia, sending the query as a text string to Google Assistant in Chrome, and searching for “Henry VIII” on the Wikipedia page.

As another example, if you ask the Google Assistant to help you purchase tickets for an upcoming movie, then the address of the website you are viewing, your credit card information, and your email address will be shared with Google to complete the transaction and make it possible for you to receive the purchase receipt and movie ticket.

If you opt-in to this feature, the Google Assistant in Chrome will send data to Google in order to complete the command you issued. When the command is issued, the Google Assistant in Chrome shares back to Google the website’s URL to validate that the webpage is allowed to be automated by Google Assistant in Chrome and to receive the instructions on how to complete the task (e.g. on how to fill out a form).

At the time the command you issued is executed, additional information can be shared. Depending on the command you issued, the information shared with Google can include the address of the website you are viewing, your email address, your name, your delivery and billing address, your credit card information, and possibly the username you use to log into the website. With the exception of email and credit card network (i.e. Visa, MasterCard, AMEX, etc.), this information is not stored by Google — rather, this information is passed on to the third party website to complete the command you issued to the Google Assistant.

To personalize future actions Google Assistant in Chrome will save configuration information about the command you issued to improve your future experiences (for example: seat selections, number and types of movie tickets, etc.). This information is saved to your Google Account.

Some Google Assistant features are not available on Incognito tabs. You can turn off the ability to use the Google Assistant in Chrome on your Android device by toggling the “Google Assistant for Chrome” option in Chrome’s settings.

Google Cloud Print

The Google Cloud Print feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google’s servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google’s servers.

A print job will be downloaded by either a Chrome browser (“Connector”) or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP’s ePrint, for example).

The print job is deleted from Google’s servers when any of three criteria is met:

- You delete the print job
- The job has been printed and marked as printed by the printer/connector
- The job has been queued on Google’s servers for 30 days

You can manage your printers and print jobs on the Google Cloud Print website.

SSL certificate reporting

Case 4:20-cv-03664-YGR Document 666-13 Filed 08/05/22 Page 77 of 83

Chrome stores locally a list of expected SSL certificate information for a variety of high-value websites, in an effort to prevent man-in-the-middle attacks. For Google websites and other websites that choose to opt in, Chrome will report a possible attack or misconfiguration. If the certificate provided by the web server doesn't match the expected signature, Chrome reports information about the SSL certificate chain to Google or to a report collection endpoint of the website's choosing. Chrome sends these reports only for certificate chains that use a public root of trust.

You can enable this feature by opting in to report data relevant to security, as described in the Safe Browsing section. While you are opted in, two kinds of reports may be sent to Google's security team. Each time you see an SSL error page, a report will be sent containing the SSL certificate chain, the server's hostname, the local time, and relevant details about the validation error and SSL error page type. Additionally, each time a mismatch between different certificate verifiers is detected, a report will be sent containing the certificate chain and the verification result.

Because Chrome sends these reports for all certificate chains, even those that chain to a private root of trust, these chains can contain personally identifiable information. You can opt out anytime by unchecking the box "Help Improve Chrome security" in "Privacy and security > More".

The SSL certificate reporting feature is not available on Chrome iOS.

Installed Applications and Extensions

Users can install external apps and extensions for the desktop versions of Chrome to add features to or customize their Chrome browsers. Installing an application or extension from the Chrome Web Store directly or via an inline installation flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you're logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google Update.

As they're more deeply integrated into Chrome, applications and extensions that you choose to install can request access to additional capabilities, enabling functionality that doesn't make sense on the web at large: background notifications or raw socket access, for instance. These additional permissions may change the way your data is collected and shared, as extensions and applications might have access to data regarding the websites you visit, and might be capable of monitoring or modifying your interactions with the web. When installing an application or extension, Chrome may first warn you about certain capabilities. Please do take the time to read and evaluate this warning before proceeding with the installation. Note also that interactions with and data collected by these third-party applications and extensions are governed by their own privacy policies, not Google's privacy policy.

Push messaging

Your device may receive push messages from the backend servers of apps and extensions installed in Chrome, websites that you grant the "notification" permission to, and your default search engine. Disabling push messages from your default search engine is done in the same way as disabling push messages from any site, by visiting the "Notifications" section of "Site settings".

Push message data is sent over a secure channel from the developer through Google's infrastructure to Chrome on your device, which can wake up apps, extensions, and websites (including your default search engine) to deliver the message. The developer may end-to-end encrypt the message data, or may send it in a form such that Google servers process it as plain text. Google servers retain up to 4 weeks' worth of messages to ensure delivery to users even if their devices are offline at the time of the initial pushing.

If the notification permission is set to "granted" for any website (including the default search engine), or you have an app or extension installed that uses push messaging, then Chrome provides the app's, extension's, or website's server with one or more registration tokens that can be used to send messages to the entity (app, extension, or website). Websites you visit in Incognito mode are not allowed to send you push messages and therefore cannot get a registration token.

When you uninstall an app or extension, revoke the notification permission for a website, or clear cookies for a permitted website, its registration token is revoked and will not be reused, even if the same app or extension is re-installed or the same website is re-visited. Registration tokens used by Chrome components such as Sync are revoked once they are no longer in use (for example, when the user disables Sync). When a registration token is revoked, the associated entity on your device stops receiving messages sent from its developer's server.

The registration tokens that are passed to entities contain an encrypted device ID, which is used for routing the messages. Google can decrypt the device ID, but other entities cannot, and the encryption is designed so that two registration tokens for the same device ID cannot be correlated. On desktop versions of Chrome, the device ID is reset when the Chrome profile is removed, or when neither Chrome Sync nor any of the entities requires it for push messaging. On Android, the lifetime of the device ID is governed by the operating system and is independent of Chrome. Any messages routed to registration tokens containing a revoked device ID will not be delivered.

Chrome custom tabs

On Android devices, an app developer may use a Custom Tab to show web content when you click on a URL from their app. A Custom Tab may look different from a regular Chrome tab, for example it may have app-specified visual style, and the absence of an editable URL bar. Despite the different visual style a Custom Tab

may have, the data sent and received in the Custom Tab, such as cookies, saved passwords and browsing history function the same way they do in a normal Chrome tab. The Custom Tab is an app-customized view using the same underlying user profile.

With Chrome Custom Tabs, an Android app developer may also specify custom actions in the Chrome toolbar and overflow menu that are relevant to their app, for example,"share", "save page", "copy URL". If you tap on such a button, the address of the current website is shared with the application.

An application can request Chrome to pre-render a given URL in the background. This allows Chrome to show you a pre-loaded site instantly when you open it from the app. At the same time it allows an application to set cookies in your browser in the background. To disable pre-rendering, you can uncheck "Preload pages for faster browsing and searching" in the privacy settings.

Trusted Web Activities are a form of Chrome Custom Tab where the top bar is not present, allowing web browsing with no browser UI but with access to the cookie jar. They can only be used to view web content on an origin that the client app can prove that it owns using [Digital Asset Links](#). If the user navigates off this origin the the top bar reappears.

When the client app is uninstalled or has its data cleared through Android Settings, Chrome will allow the user to clear data for the linked origin.

Continue where you left off

If you have selected the option to "Continue where you left off" in settings on desktop versions of Chrome, when you open Chrome, it attempts to bring you right back to the way things were when the browser was closed. Chrome reloads the tabs you had open and persists session information to get you up and running as quickly as possible. This feature effectively extends a browsing session across restarts. In this mode, session cookies are no longer deleted when the browser closes; instead, they remain available on restart to keep you logged into your favorite sites.

On desktop versions of Chrome, this feature can be enabled or disabled in Chrome settings. On Chrome OS, it is enabled by default.

On OS X, when you restart your device, a checkbox in the OS confirmation dialog asks you whether you want to re-open applications and windows after restart. If you check this box, Chrome restores tabs and windows, as well as the session cookies, even if you have disabled "Continue where you left off" on Chrome.

On mobile versions of Chrome, this feature is always enabled without a setting.

Chrome Variations

Chrome is constantly evolving to better meet the needs of users and the web. To ensure new features are providing the best experience and working correctly, they may be enabled for a subset of users before they are fully launched. For example, if we improve how page loading works in Chrome, we may try it out for 1% of users to ensure that it doesn't crash or run slower before launching to everyone. This is done through a system called "Chrome Variations" - also known as "field trials".

A given Chrome installation may be participating in a number of different variations (for different features) at the same time. These fall into two categories:

1. Low entropy variations, which are randomized based on a number from 0 to 7999 (13 bits) that's randomly generated by each Chrome installation on the first run.
2. High entropy variations, which are randomized using the usage statistics token for Chrome installations that have usage statistics reporting enabled.

Other factors may additionally inform the variations assigned to a Chrome installation, such as country (determined by your IP address), operating system, Chrome version and other parameters.

Usage statistics and crash reports are tagged with all variations a client participates in, including both low entropy and high entropy variations. These reports, which also contain a pseudonymous client identifier, can be disabled in Chrome settings.

Additionally, a subset of low entropy variations are included in network requests sent to Google. The combined state of these variations is non-identifying, since it is based on a 13-bit low entropy value (see above). These are transmitted using the "X-Client-Data" HTTP header, which contains a list of active variations. On Android, this header may include a limited set of external server-side experiments, which may affect the Chrome installation. This header is used to evaluate the effect on Google servers - for example, a networking change may affect YouTube video load speed or an Omnibox ranking update may result in more helpful Google Search results.

You can reset the variations used by your Chrome installation by starting it with the "--reset-variation-state" command line flag.

Do Not Track

If you enable the “Do Not Track” preference in Chrome’s settings, Chrome will send a DNT:1 HTTP header with your outgoing HTTP, HTTPS and SPDY browsing traffic (Chrome cannot, however, guarantee that NPAPI plugins also send the header.) The header will not be sent with system traffic such as the geolocation, metrics or device management services.

The effect of Do Not Track depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example, to improve security; to provide content, services, ads and recommendations on their websites; and to generate reporting statistics.

Chrome on iOS now uses WKWebView to provide a more stable and faster browser. As a result of this move, the Do Not Track preference is no longer available due to iOS constraints. If Apple makes changes to allow this feature, Chrome will make Do Not Track available again in iOS.

Plugins

Chrome ships with an Adobe Flash Player implementation that is based on the Pepper API. Flash and other Pepper-based plugins may ask you for “Access to your computer”. If you grant this permission, the plugin is granted unsandboxed access. This allows content providers to offer you access to DRM protected content like videos or music but may have security and privacy implications, so consider carefully whether you trust a plugin or website with this privilege.

Media licenses

Some websites encrypt media to protect against unauthorized access and copying. When users play media from these sites, they typically log into the site, which authenticates the user, and then digital rights management negotiates a key exchange for the decryption and playback of the media.

For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. The implementation of that API is tightly coupled with the browser to protect user privacy and security, through Content Decryption Modules (CDM), which are provided by digital rights management solutions such as Google Widevine or Microsoft PlayReady.

When a user asks Chrome to play encrypted HTML5 media (for example, watching a movie on Google Play Movies), Chrome will generate a request for a license to decrypt that media. This license request contains an automatically generated request ID, which is created by the Content Decryption Module, as well as proof that the CDM is legitimate. After generation, the license request is typically sent to a license server managed by either the content website or Google. Neither the license request, the proof, nor the request ID include any personally identifying information. After being sent, the license request is not stored locally on the user's device.

As part of the license request, Chrome also generates a unique session ID which does not contain personally identifying information. This session ID is sent to the license server, and when the server returns a license the session ID is used to decrypt the media. The session ID may be stored locally even after the site has been closed. The license may also be stored locally for offline consumption of protected content. Session ID and licenses may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

When returning a license, the site license server may include a client ID, generated by the site. This client ID is unique to the user and the site, it is not shared between sites. If provided, the client ID is stored locally and included by Chrome in subsequent license requests to that site. The client ID may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

On some platforms, the website may additionally request verification that the device is eligible to play specific types of protected content. On Chrome OS, this is known as [Verified Access](#). In this case, Google creates a certificate using a unique hardware identifier for the device. This hardware ID identifies the device, but does not identify the user. If the user agrees, Google receives the hardware ID and generates a certificate verifying the device for the requested site. The certificate does not include the hardware ID or any other information that could permanently identify the device. Certificates are stored locally similar to other cached browsing data, and may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected. On Android, this is called [Provisioning](#). See “[MediaDrm Provisioning](#)” for more details.

Some sites use Flash instead of HTML5. If a website you visit chooses to use Adobe Flash Access DRM protection, Chrome for Windows and Chrome OS will give Adobe Flash access to a device identifier. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with “Cookies and other site data” selected.

In order to give you access to licensed music, the [Google Play Music app](#) can retrieve a device identifier that is derived from your hard drive partitions or, on a Chrome OS or Linux installation, from a unique file on your disk. This identifier can be reset by reinstalling your operating system.

MediaDrm provisioning

Chrome on Android uses [Android MediaDrm](#) to play protected content. As on ChromeOS, the website may request verification that the device is eligible to do so. This is achieved by MediaDrm provisioning. A provisioning request is sent to Google, which generates a certificate that will be stored on the device and sent to the

Case 4:20-cv-03664-YGR Document 666-13 Filed 08/05/22 Page 80 of 83

site whenever you play protected content. The information in the provisioning request and in the certificate vary depending on the Android version. In all cases, the information can be used to identify the device, but never the user.

On Android K and L, the device only needs to be provisioned once and the certificate is shared by all applications running on the device. The request contains a hardware ID, and the certificate contains a stable device ID, both of which could be used to permanently identify the device.

On Android M or later, MediaDrm supports per-origin provisioning. Chrome randomly generates an origin ID for each website to be provisioned. Even though the request still contains a hardware ID, the certificate is different for each website, so that different websites cannot cross-reference the same device.

On Android O or later on some devices, provisioning can be scoped to a single application. The request will contain a hardware ID, but the certificate will be different for each application, in addition to each site, so different applications cannot cross-reference the same device.

Provisioning can be controlled by the “Protected media” permission in the “Site settings” menu. On Android versions K and L, Chrome will always ask you to grant this permission before provisioning starts. On later versions of Android, this permission is granted by default. You can clear the provisioned certificates anytime using the “Cookies and other site data” option in the [Clear browsing data](#) dialog.

Chrome also performs MediaDrm pre-provisioning to support playback of protected content in cases where the provisioning server is not accessible, such as in-flight entertainment. Chrome randomly generates a list of origin IDs and provision them in advance for future use.

On Android versions with per-device provisioning, where provisioning requires a permission, Chrome does not support pre-provisioning. Playback might still work because the device could have already been provisioned by other applications.

On Android versions with per-origin provisioning, Chrome pre-provisions itself once the user attempts to play protected content. As the provisioning for the first playback already involved sending a stable hardware ID to Google, the subsequent pre-provisioning of additional origin IDs introduces no new privacy implications. If provisioning fails and there is no pre-provisioned origin ID, Chrome may ask for permission to further fallback to per-device provisioning.

On devices with per-application provisioning, Chrome pre-provisions itself automatically on startup.

Cloud policy

When you sign into a Chrome OS device, Chrome on Android, or a desktop Chrome profile with an account associated with a Google Apps domain, or if your desktop browser is enrolled in Chrome Browser Cloud Management, Chrome checks whether the domain has configured enterprise policies. If so, the Chrome OS user session, Chrome profile, or enrolled Chrome Browser is assigned a unique ID, and registered as belonging to that Google Apps domain. Any configured policies are applied. To revoke the registration, remove the Chrome OS user, sign out of Chrome on Android, remove the desktop profile, or [remove the enrollment token and device token](#) for Chrome Browser Cloud Management.

Additionally, Chrome OS devices can be enrolled to a Google Apps domain by a domain admin. This will enforce enterprise policies for the entire device, such as providing shared network configurations and restricting access to developer mode. When a Chrome OS device is enrolled to a domain, then a unique device ID is registered to the device. In order to revoke the registration, the admin will need to wipe the entire Chrome OS device.

Registered profiles and devices check for policy changes periodically (every 3 hours by default). In some cases, the server pushes policy changes to the client without waiting for Chrome's periodic check. Unregistered profiles check whether a policy has been turned on for their domain each time Chrome starts up.

The [policy list](#) contains details about the types of configurations that are available via Cloud Policy.

Lite Mode

If you enable Lite Mode, Chrome will send your traffic through Google's optimizing proxy servers. This option reduces the amount of data downloaded and speeds up your page loads. This feature was previously known as “Data Saver”.

Most of the time, only your HTTP traffic is transparently proxied, and you won’t notice any changes to the page. However, if Chrome anticipates the page will load especially slowly, both HTTP and HTTPS pages will be optimized to load faster. For HTTPS origins, the transcoded pages are served from a Google-owned domain instead of being transparently proxied. Because these pages are served from a Google-owned domain instead of the original domain, Chrome will not send any origin-scoped information (e.g., cookies or data from local storage) for the original domain to Google, and Google cannot set any origin-scoped information for the original domain in Chrome. Pages loaded in Incognito are never proxied or optimized by Lite Mode.

Additionally, when you enable Lite Mode, Chrome may share the URLs and usage and performance statistics of the websites you visited with Google in order to identify the websites that load slowly and improve their performance.

Request URLs are logged, but Cookie and If-None-Match headers are stripped from the logs (and cookies are never seen in the case of HTTPS pages). Additionally, the content of proxied pages is cached but not logged. The logs are not associated with your Google Account, and the entire log entry is removed within 14 days. These logs are also governed by standard Google search logging policies.

Google uses the logged and cached data to improve both Lite Mode and Safe Browsing; for example, more effective optimizations can be uncovered by analyzing timing data for pages loaded through the proxy service, and malware can be detected more rapidly by analyzing response data in realtime.

Your IP address is forwarded to the origin HTTP server via an X-Forwarded-For header, in accordance with the HTTP standard. The Lite Mode service is a transparent proxy, *not* an anonymization service.

By default, the connection between the browser and the Lite Mode proxy is over an encrypted channel. However, a network administrator can disable the use of an encrypted channel to Lite Mode.

To further improve loading performance for Lite mode users, if you have the “Preload pages for faster browsing and searching” setting enabled, Chrome may prefetch search result links found on the Google Search page. Four mechanisms preserve user privacy for these prefetches:

- Prefetching is disabled if Chrome has a cookie for the domain.
- Passive fingerprinting surfaces such as User-Agent are bucketed or set to fixed values.
- Prefetches are tunneled through a CONNECT proxy operated by Google, and only HTTPS links are prefetched. Consequently, the TLS connection is established between Chrome and the origin so the proxy server cannot inspect the traffic, and requests to the origin come from a Google IP instead of the user’s IP. Google only learns about the destination domain that will be prefetched, which Google already knows as it generated the Search results page.
- Prefetched resources and cookies set by the prefetched domain are only persisted when you click the search result and visit the prefetched domain.

Using Chrome with a kid’s Google Account

Chrome for Android offers features to be used when signed in with a kid's Google Account and automatically signs in a kid's account if they've signed into the Android device. Chrome uses the Sync feature to sync settings configured by parents to the kid’s account. You can read about how Sync data is used in the Sign in section of this Whitepaper.

The collection and use of Chrome data in association with a kid’s Google Account are governed by the Google Family Link - Children’s Privacy Policy.

In order for the configured settings to apply to a kid’s account, Chrome does not support the following features for a kid’s Google Account: signing out of Chrome, Incognito mode, and deleting browsing history from within Chrome. Browsing history can still be removed in the Chrome section of the Google Dashboard.

By default, first party cookie blocking is disabled when Chrome is signed in with a kid’s account. Parents can go to chrome.google.com/manage/family to allow their kids to block first party cookies. However, blocking cookies signs kids out of Google web products such as Google Search or YouTube and therefore prevents these products from providing any features designed for kids’ Google Accounts.

When Chrome is used with a kid’s Google Account, information about the kid’s requests to access blocked content is sent to Google and made visible to the kid’s parent(s) on chrome.google.com/manage/family and in the Google Family Link app. If the kid’s browsing mode is set to “Try to block mature sites”, Chrome will send a request to the Google SafeSearch service for each navigation in order to block access to sites that have been classified as containing mature content.

Incognito and Guest Mode

Incognito mode in Chrome is a temporary browsing mode. It ensures that you don’t leave browsing history and cookies on your computer. The browsing history and cookies are deleted only once you have closed the last incognito window. Incognito mode cannot make you invisible on the internet. Websites that you navigate to may record your visits. Going incognito doesn’t hide your browsing from your employer, your internet service provider, or the websites you visit.

Browsing as a Guest in Chrome allows you to use somebody else's computer without modifying their profile. For example, no bookmarks or passwords get stored on their computer. Note that Guest mode does not protect you for example, if the computer you are using is infected by a keylogger that records what you type.

iOS 8 and Mac OS X Yosemite Handoff Support

While browsing in a standard (i.e. non-Incognito) session, Chrome will share your current URL with iOS 8+ to support the Handoff feature that was added in OS X Yosemite. This information is only sent to Apple devices that are paired with your iOS device, and the data is encrypted in transit.

More information is available at Apple Support, Apple Developers, and in the Apple iOS Security Guide. Chrome support for this feature can be disabled in Chrome settings.

A FIDO U2F Security Key provides a non-phishable credential which can be used to authenticate a user. This mitigates the risk of various kinds of man-in-the-middle attacks in which websites try to steal your password and use it later.

To prevent abuse, a website is required to be delivered over a secure connection (HTTPS), and to register the security key before it can be used for identification. Once a website is registered with a specific security key, that security key will provide a persistent identifier, regardless of which computer it is plugged into, or whether you're in incognito or guest mode, but you must physically interact with the security key to give a website access to an identifier (by, for example, touching it, or plugging it in).

Physical Web

The Physical Web lets you see a list of URLs being broadcast by objects in the environment around you. Google Chrome looks for Physical Web devices with Bluetooth Low Energy beacons that are broadcasting URLs using the Eddystone protocol. Bluetooth signals can be received from 90 feet away or more, depending on signal strength and the user's environment (although the range is often much shorter, due to obstacles and signal noise). If the Physical Web feature is enabled, Chrome sends detected URLs to Google's Physical Web Service (PWS) via a cookieless HTTPS request. For each URL, the PWS obtains the title of the web page, filters out unsafe results, and returns a ranking based on non-personalized signals about the quality and relevance of the web page.

The Physical Web feature is available on Chrome on iOS and Android. Users will need to turn on Bluetooth to use the feature.

If Android users have location settings enabled on both their device and in Chrome, they will receive a notification the first time they are near a beacon that will give them the option to turn on the Physical Web feature. This beacon's URL is not sent to Google's PWS unless the Physical Web feature is enabled. Users can also enable (or disable) the feature in the Privacy settings. Once a user enables the feature, Chrome scans for nearby devices for a few seconds each time the user unlocks the mobile device in use and sends them to the PWS in order to obtain more information about the beacon. The user receives a silent notification when Chrome finds a nearby URL.

On iOS devices, users can enable (or disable) the feature in the Privacy settings or by adding the Chrome widget to their Today view in the notification center. Additionally, the feature is automatically enabled for users who have location enabled on their device, granted Chrome the location permission, and have granted Google the geolocation permission. Chrome scans for nearby devices whenever it is open in the foreground. When Chrome finds nearby URLs, users will see them as omnibox suggestions. Additionally, Chrome scans for nearby devices for a few seconds when the Today widget is displayed in the notification center.

Bluetooth

Google Chrome supports the Web Bluetooth API, which provides websites with access to nearby Bluetooth Low Energy devices with your consent.

Chrome does not let any page communicate with a device unless you explicitly consent. When a web page asks to pair with a device, Chrome will ask you to choose which device the web page should access, if any. Selecting a device for one page does not give other pages access to the device you have chosen, and does not allow that page to access other devices. Currently, permission for a page to communicate with a device is usually revoked when the page is reloaded, and is always revoked when Chrome is restarted.

Chrome data that Android sends to Google

The data collection and usage described in this section is handled by Android and governed by the Google Privacy Policy.

If the Android Backup Service is enabled on your device, some of your Chrome preferences will be saved and stored on Google servers. For Nexus and Android One devices, it is described under "Back up your data and settings with Android Backup Service" in this article. For other Android devices, you may be able to find help by looking up your device on this page. When setting up a new Android device, you may request that it copies the preferences from a previously set up device. If you do so, Android may restore backed up Chrome preferences when Chrome is first installed. The new device only copies the preferences if automatic restore is enabled (see "Restore your data and settings" in the same article), Chrome was signed into an account when the backup was made, and the new Android device is signed into that same account.

Chrome's backup data for a particular device may also be restored if you uninstall and then later re-install Chrome on that device. This will only happen if automatic restore is enabled and the device is signed into the account that Chrome was signed into when the backup was made.

Integration with Digital Wellbeing

If you opt-in to see sites you have visited and set site timers in the Digital Wellbeing app on Android, Chrome will report which websites you've visited and the length of time spent in each of them to the app. Sites visited in incognito mode will not be reported to the Digital Wellbeing app.

To continually improve the experience of Digital Wellbeing, the app will share with Google the websites that you set a timer on and how long you have visited them.

You can opt out of this feature in the Digital Wellbeing app or in Chrome’s privacy settings anytime.

Follow us



Chrome Family

Other Platforms

Chromebooks

Chromecast

Chrome Cleanup Tool

Enterprise

Download Chrome Browser

Chrome Browser for Enterprise

Chrome Devices

Chrome OS

Google Cloud

G Suite

Education

Google Chrome Browser

Devices

Web Store

Dev and Partners

Chromium

Chrome OS

Chrome Web Store

Chrome Experiments

Chrome Beta

Chrome Dev

Chrome Canary

Stay Connected

Google Chrome Blog

Chrome Help



Privacy and Terms

About Google

Google Products



Help